“opinionway pour CESIN

Corporate Cybersecurity Barometer

Wave 8 - January 2023

Press contact:
Véronique LOQUET - ***AL'X COMMUNICATION***
06 68 42 79 68 - vloquet@alx-communication.com

Context

Context and objectives

- The ***Club des Experts de la Sécurité de l'Information et du Numérique*** (CESIN) provides a forum for **security and digital experts** within large companies.

- CESIN partnered with OpinionWay to launch its first major survey of its members in 2015 in order to learn about:
  - the **perception of cybersecurity and its challenges** within CESIN member companies
  - **the** practical **reality** of IT security in large companies.

- The survey, which is repeated every year, updates results on the perception and reality of cybersecurity, and provides new data on the impact of the digital transformation of companies.

Methodology

Methodology

Sample of **328 CESIN members,** from the CESIN members' file.

Questionnaire

The sample group was interviewed by **online self-administered questionnaire on a CAWI** (Computer Assisted Web Interview) system.

The interviews were conducted **from 8 December 2022 to 10 January 2023**

OpinionWay carried out this survey in accordance with the procedures and regulations set out in **ISO standard 20252**

The results of this survey must be read taking margins of error into account: 5.5 points at most for a sample of 330 respondents.

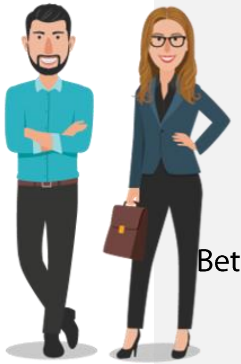
Any total or partial publication of this survey must include the following complete statement:

"OpinionWay survey for CESIN"

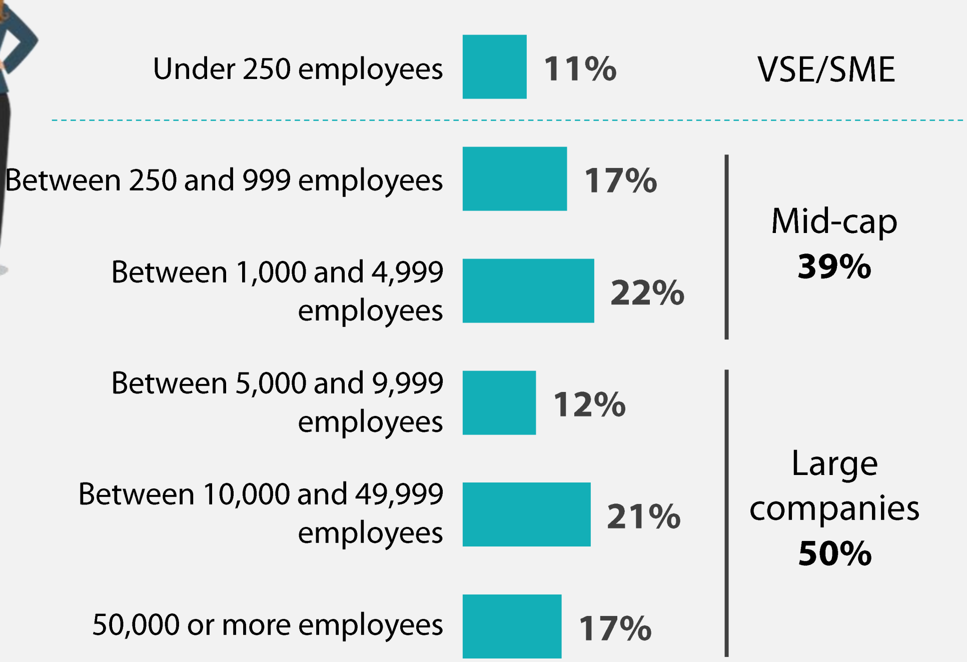
and any repeat of the survey cannot be dissociated from this title.

Sample

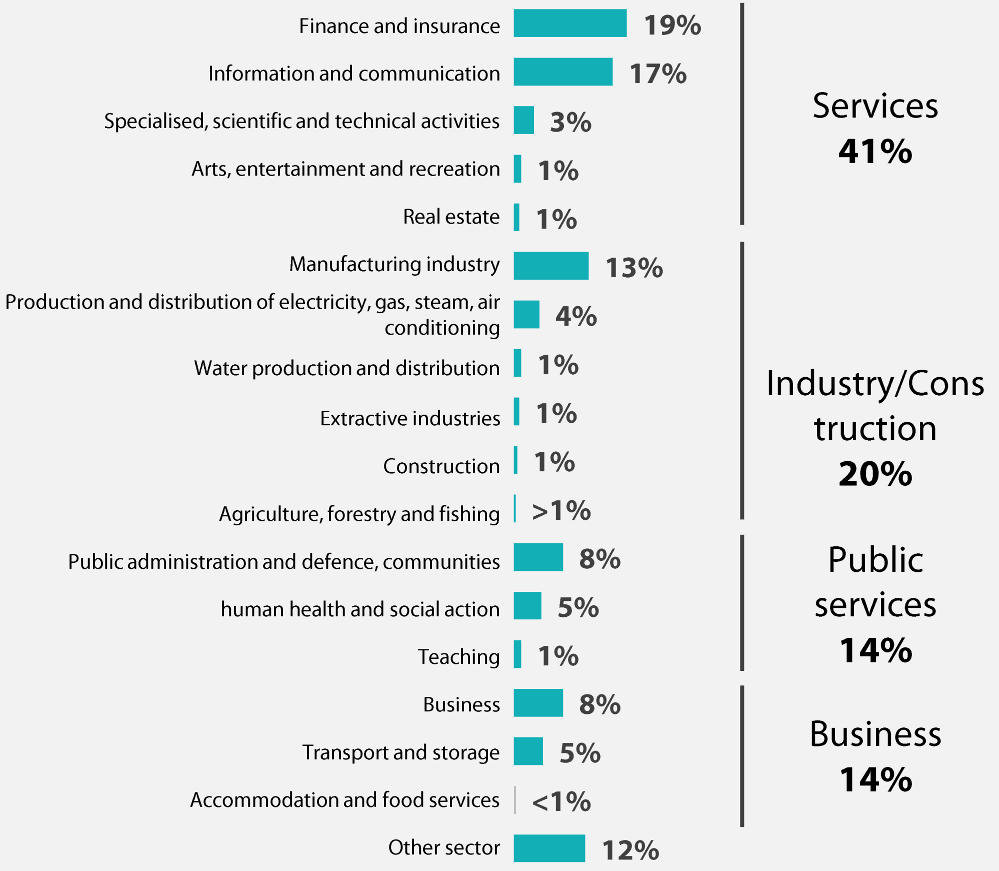
A sample that fully reflects the diversity of the population surveyed



Number of employees in the company



Business activity sector



Analyse

01

A drop in the number of successful cyberattacks in 2022...

CESIN definition of “cyberattack” clarified for this wave *

“A cyberattack, for the purposes of this survey, is the occurrence of a malicious act against an IT device that significantly impairs the confidentiality and/or integrity of the company’s information or the availability of the information system, resulting in significant financial loss and/or damage to the company’s image and/or significant defence efforts to contain and deal with the attack. This does not include attempted attacks that have been stopped by your prevention systems”

***Definition in wave 6**: A cyberattack, for the purposes of this survey, is when a malicious act is performed against a computer device that significantly affects the confidentiality and/or integrity of the company’s information or the availability of the information system, resulting in significant financial losses and/or damage to the company’s image.*

Fewer than 1 in 2 companies have suffered a successful cyberattack this year, a proportion that is down on 2021 (-9 pts)

328 people

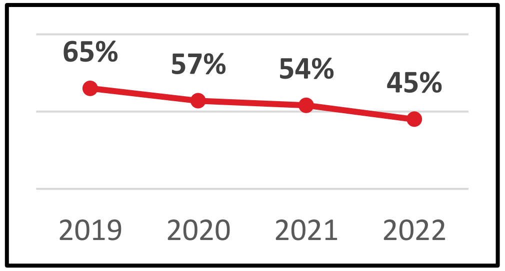
Q4. In general, how many significant cyberattacks has your company suffered in the last 12 months?

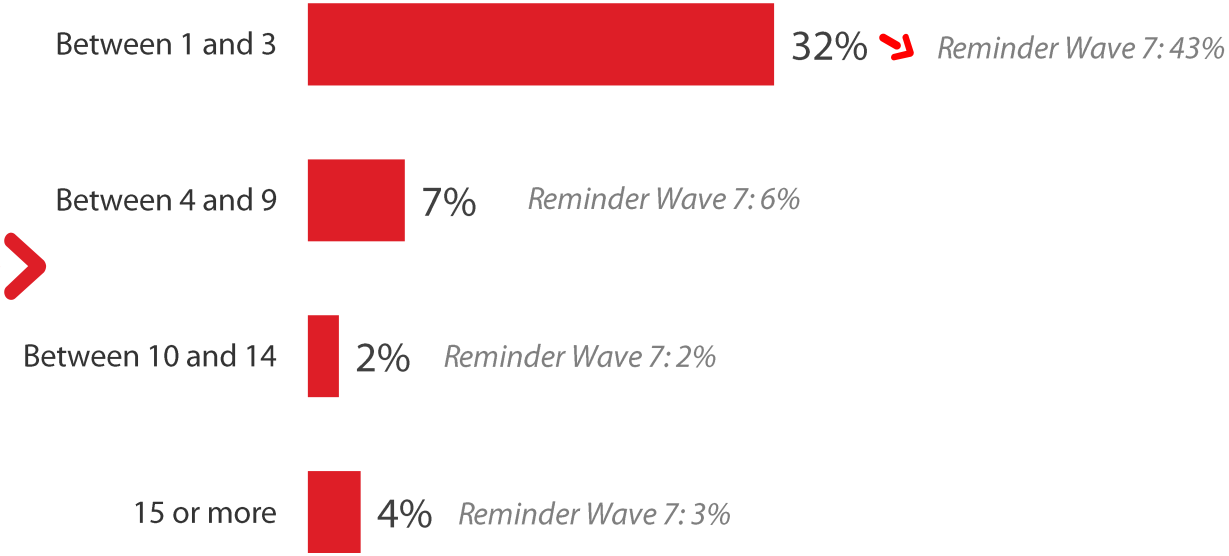
All respondents

45% ↘ -9

of companies have experienced at least one cyberattack

Reminder





↗ ↘ Statistically significant change compared to the previous wave

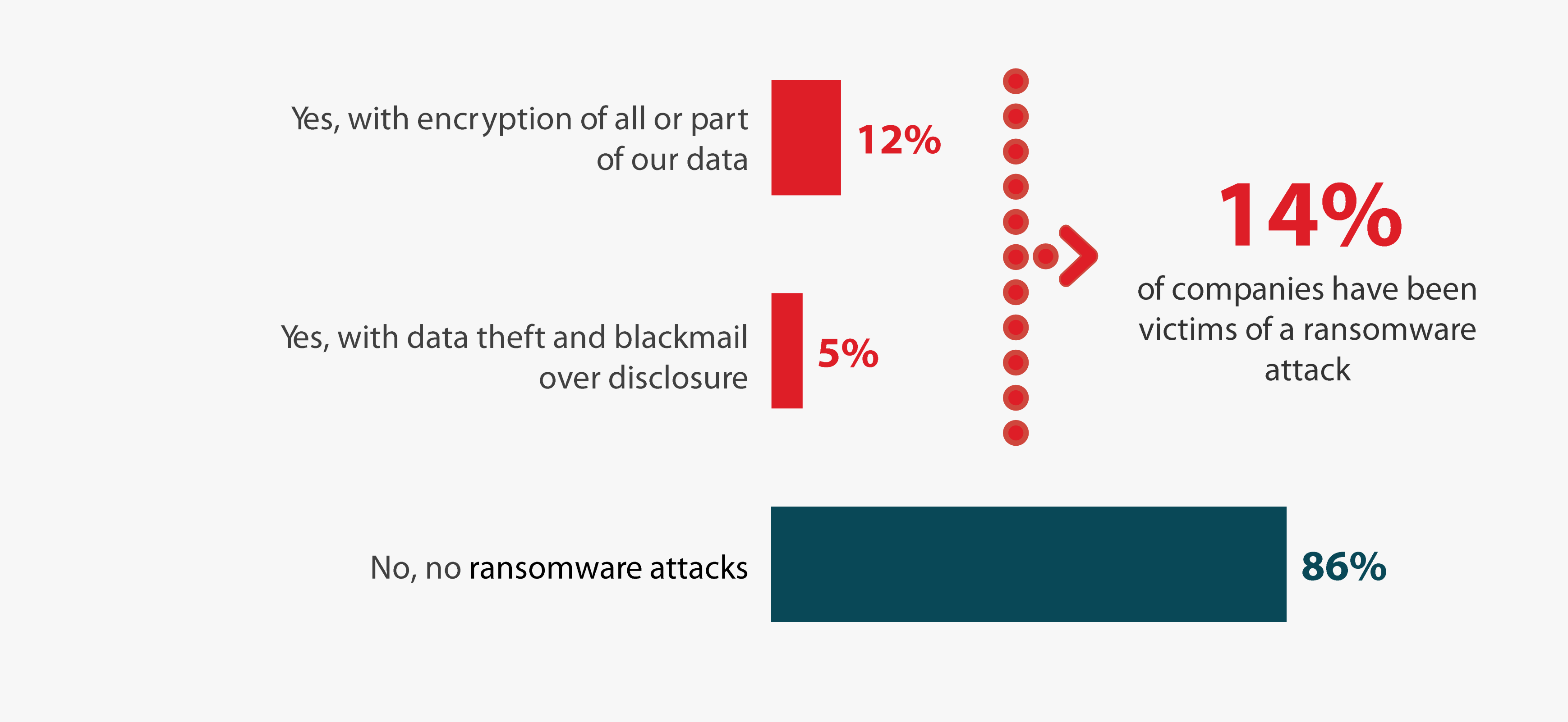
Less than 1 in 5 companies have fallen victim to ransomware, a figure that is set to fall in relation to 2021

328 people

Last year was again marked by an increase in the ransomware threat. In addition to the wave of successful attacks in some cases, attackers have made blackmail threats over data disclosure.

Q10. Have you been a victim of a ransomware attack?

All respondents/Several answers possible



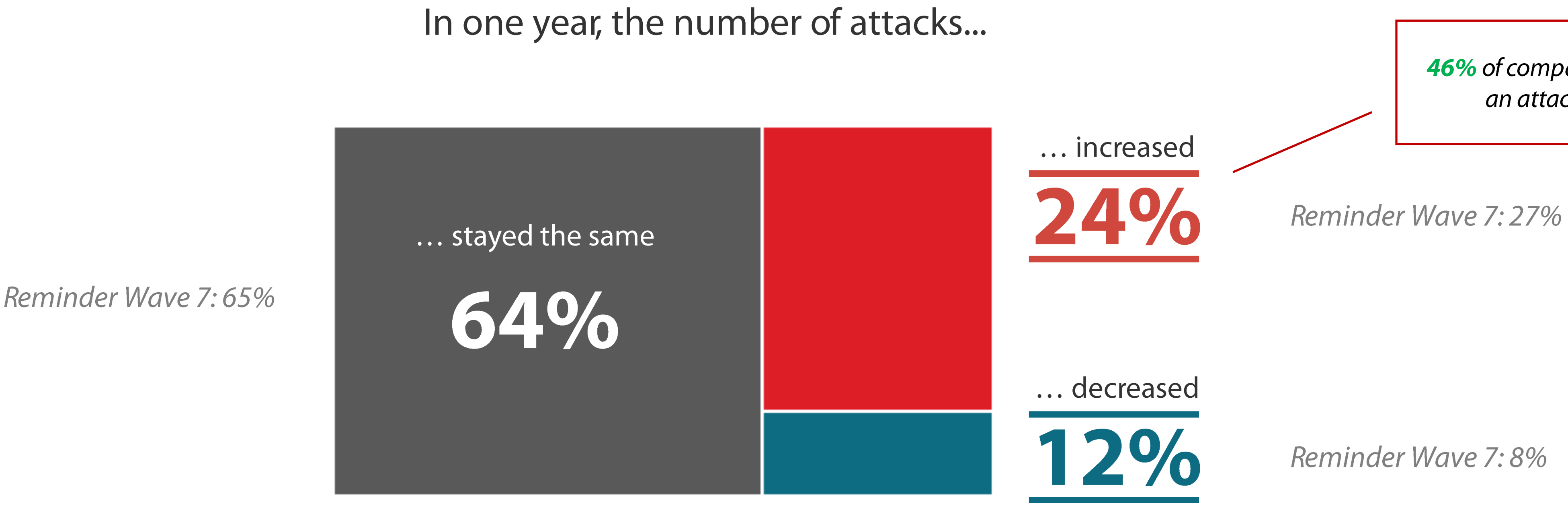
Reminder Wave 7: 18%

While the number of attacks compared to last year seems to remain stable, a significant proportion still believe that they have increased

328 people

Q4a. And compared to last year, the number of observed attacks in your company has...?

All respondents



46% of companies reporting an attack in 2022

↗ ↘ Statistically significant change compared to the previous wave

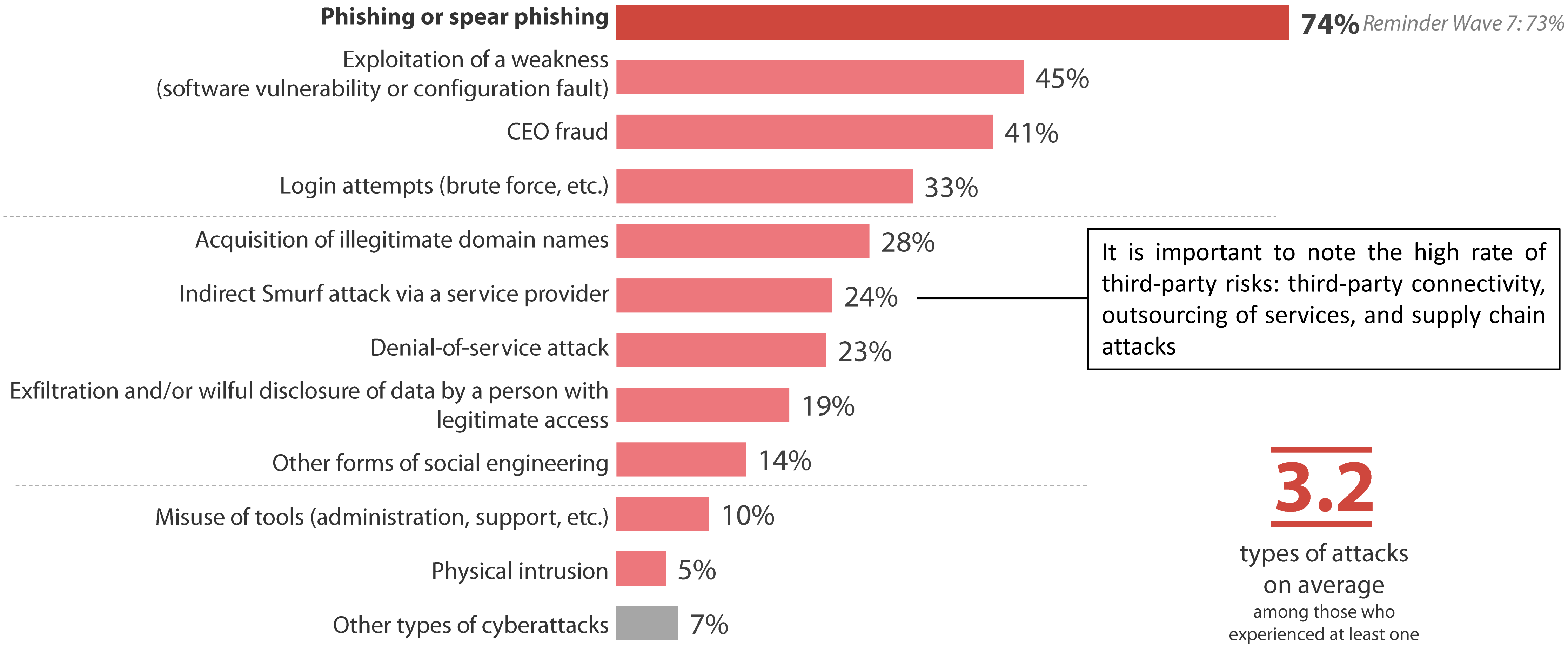
Companies that have experienced at least one attack have suffered an average of three, with phishing or spear phishing clearly the main vector

147 people

Q5a. Which of the following attack vectors have impacted your company in the last 12 months?

Respondents having noticed an attack/Several answers possible

45% of companies suffered at least one cyberattack in 2022



It is important to note the high rate of third-party risks: third-party connectivity, outsourcing of services, and supply chain attacks

3.2

types of attacks on average

among those who experienced at least one attack

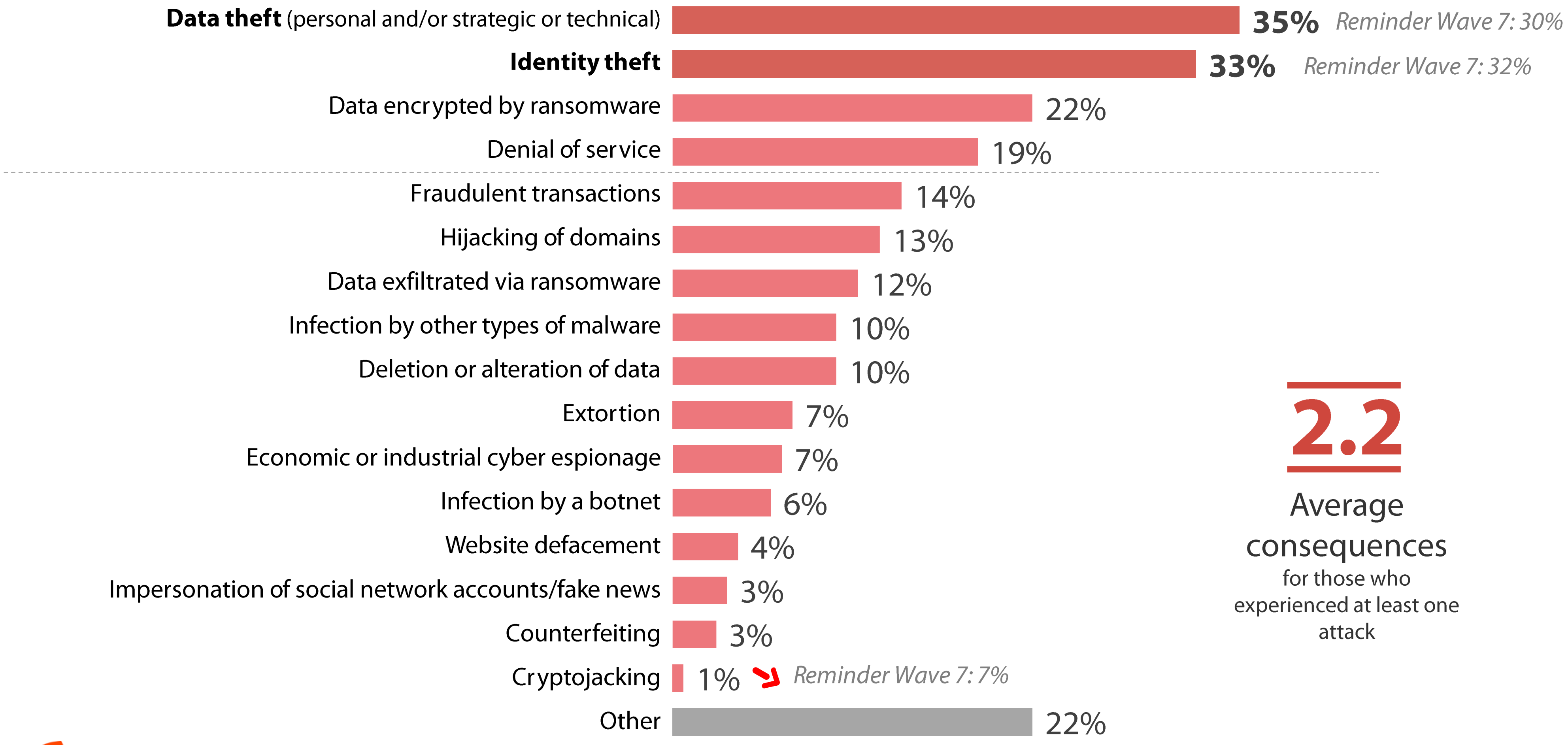
Data theft and identity theft remain the major consequences for companies

147 people

Q5b. And what were the consequences of this/these attack(s)?

Respondents having noticed an attack/Several answers possible

45% of companies suffered at least one cyberattack in 2022



2.2

Average consequences

for those who experienced at least one attack

↗ ↘ Statistically significant change compared to the previous wave

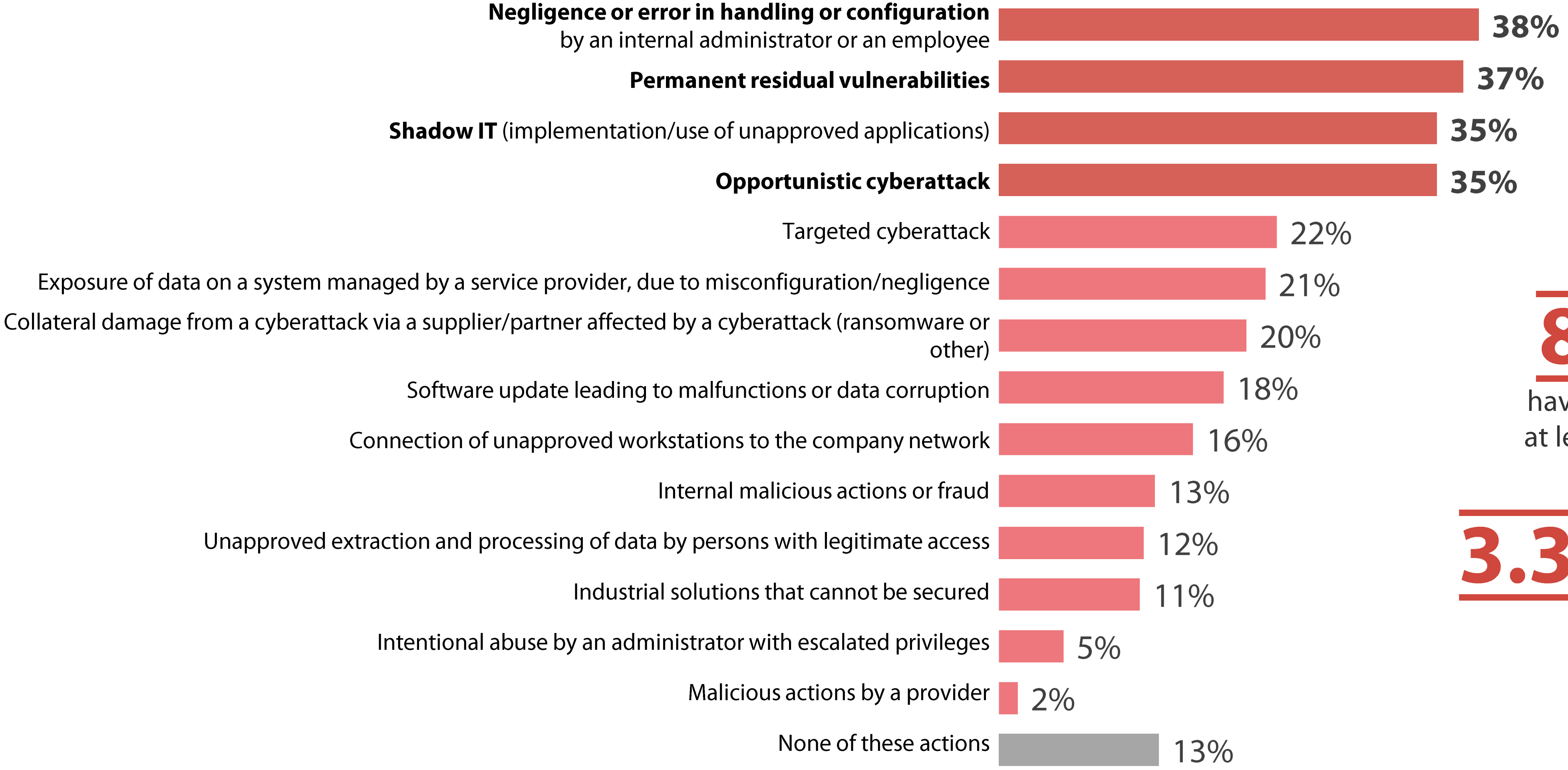
“opinionway for CESIN

The main causes of security incidents lie in the lack of respect for fundamental IT practices, vulnerability management and Shadow IT

328 people

Q6. Among the causes of security incidents encountered by the company, including cyberattacks, which ones has your company actually faced in the last 12 months?

All respondents/Several answers possible



87%
have experienced at least one action

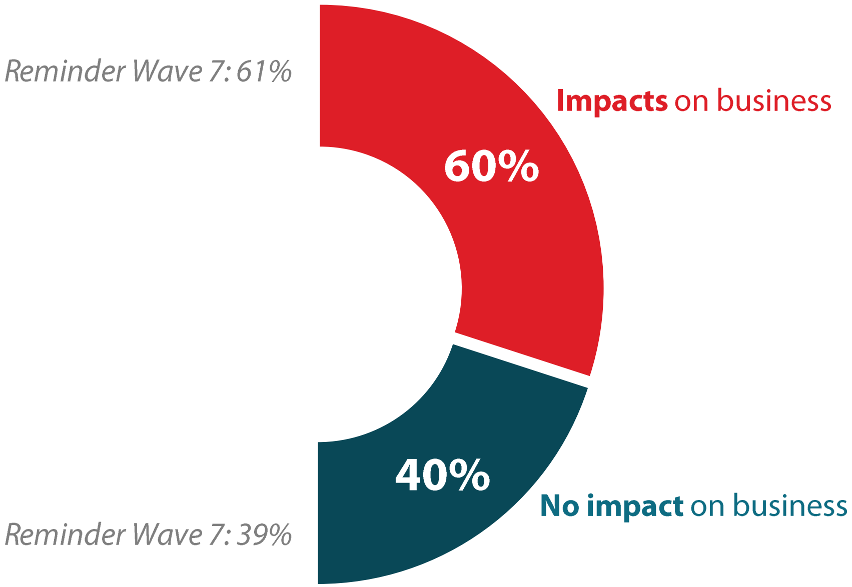
3.3 actions on average

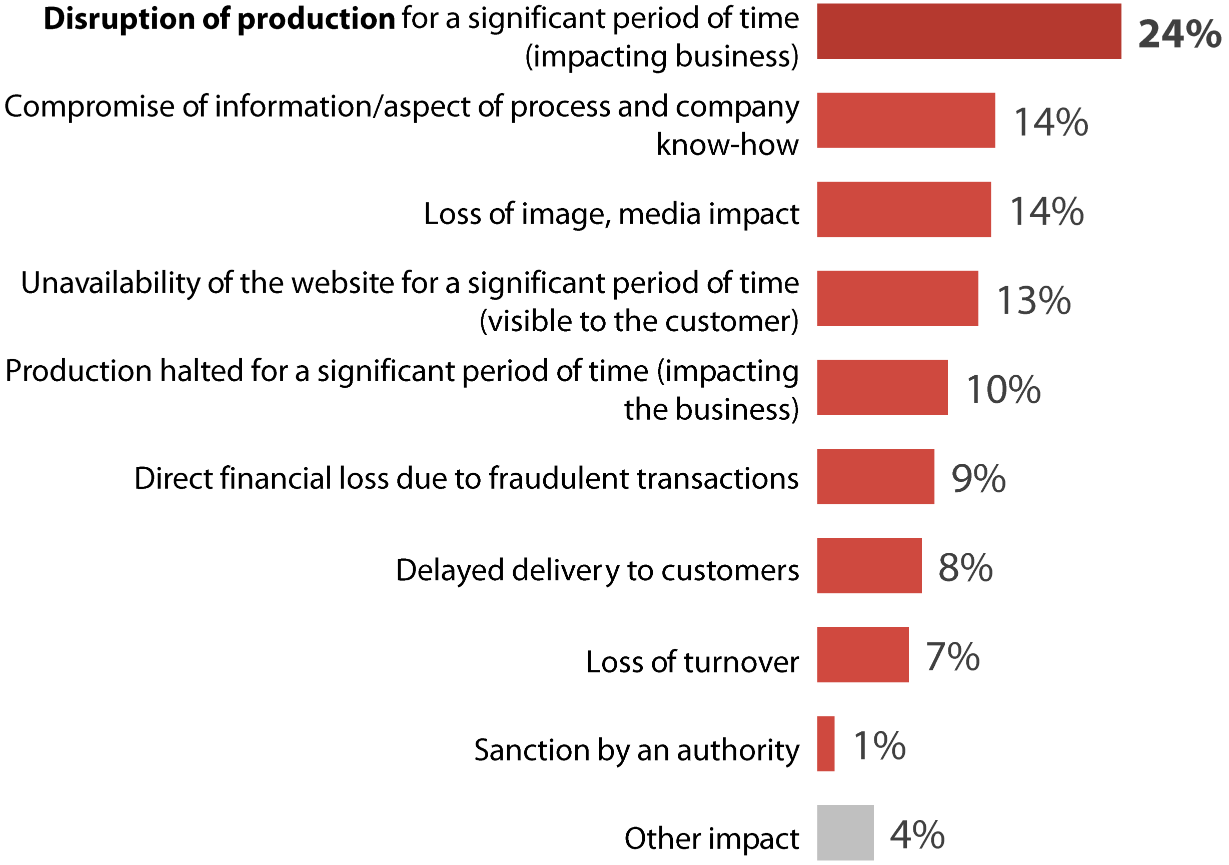
As in 2021, 6 out of 10 companies noted an impact of cyberattacks on their business, including a disruption of their production

292 people

Q7. What has been the impact of cyberattacks on your business?

Respondents having observed an attack and a cause of security incidents/Several answers possible



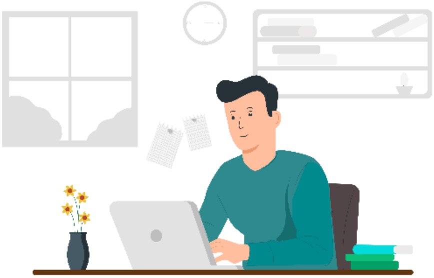


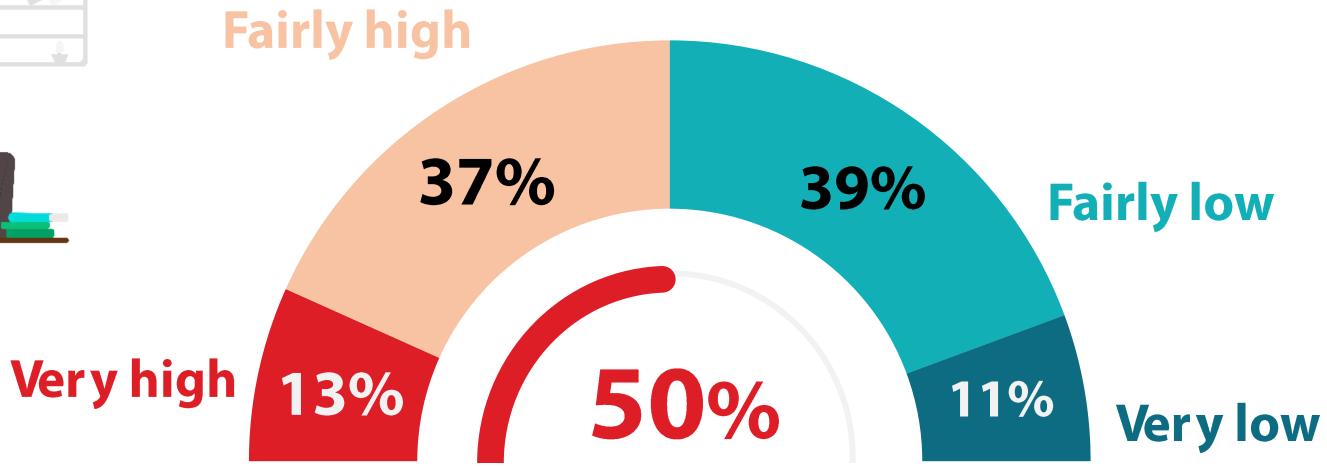
The level of cyber espionage threats is perceived as high by one in two companies, a figure that is stable compared to last year

328 people

Q9. Today, how do you assess the level of cyber-espionage threats to your company?

All respondents





ASSESS A HIGH LEVEL OF CYBER ESPIONAGE THREATS

Reminder Wave 7: 55%

02

...which can be explained by greater protection of companies

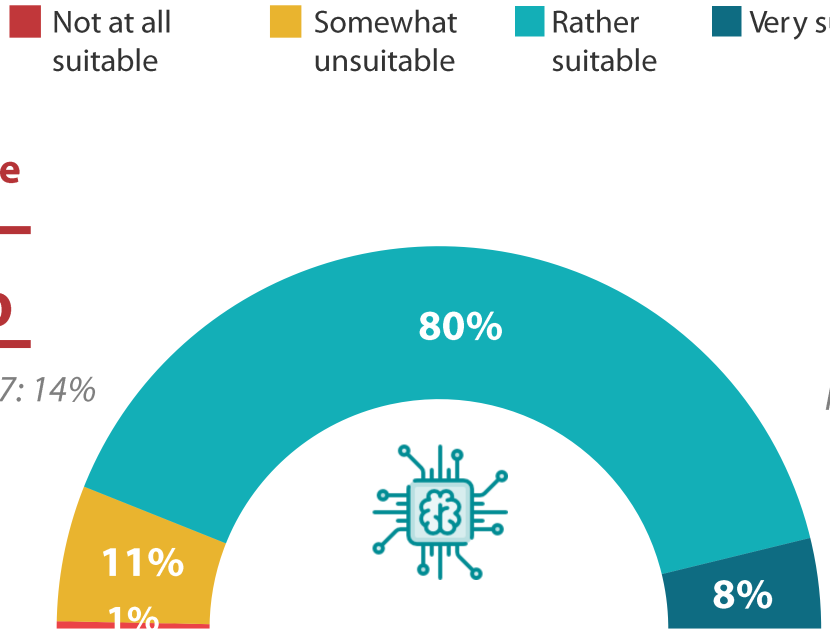
Confidence in the solutions and services available on the market is growing over the years

328 people

Modified question

Q25. Do you think that the security solutions available on the market are very suitable, somewhat suitable, somewhat unsuitable or not at all suitable for your company?

All respondents



% Unsuitable

12%

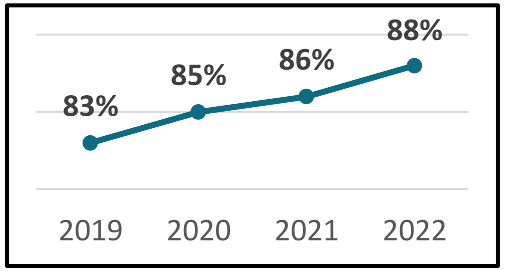
Reminder Wave 7: 14%

% Suitable

88%

Reminder Wave 7: 86%

Reminder



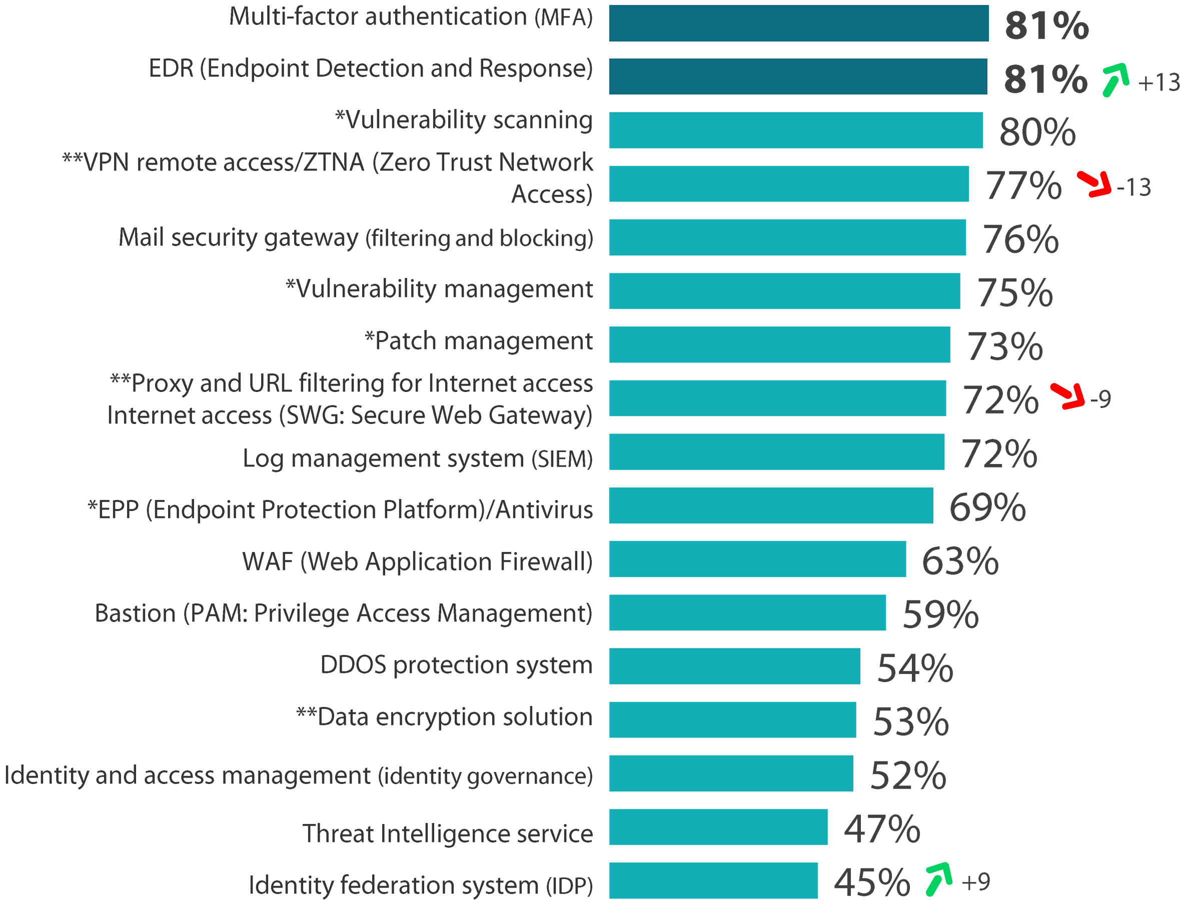
On average, companies have implemented close to 15 solutions or services. There is an increasing emphasis on detection and rapid detection and response tools (EDR/NDR) and orchestration tools (SOAR)

328 people

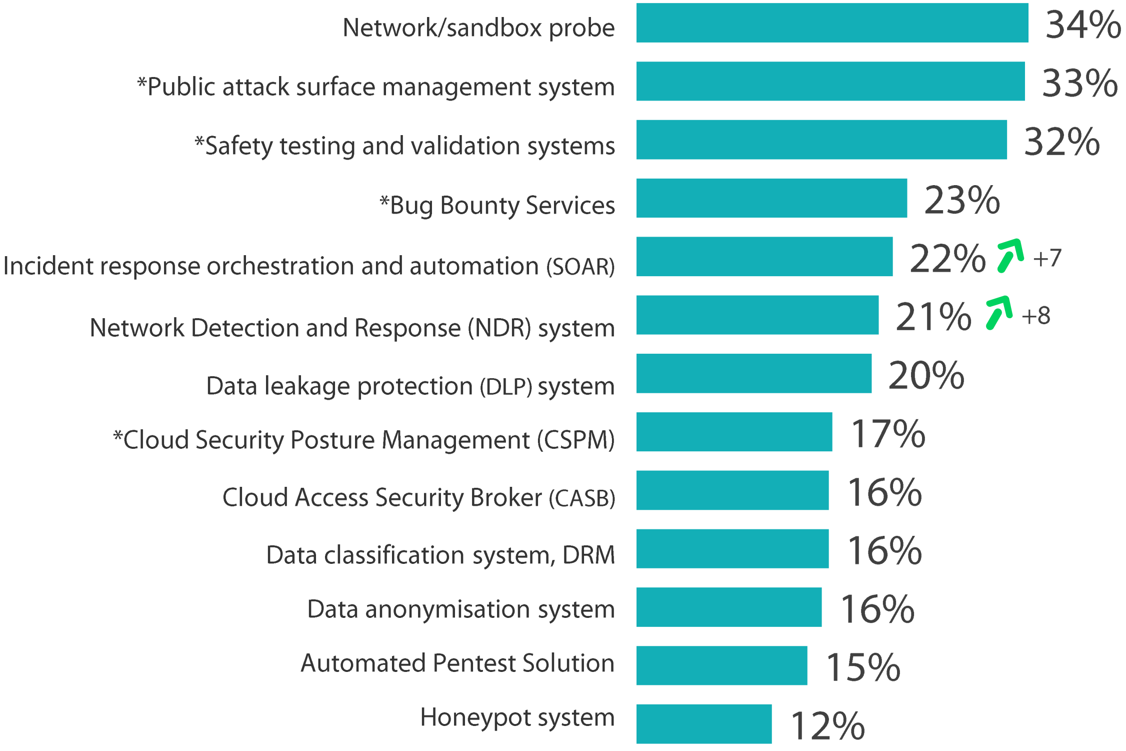
Modified question

Q12. More generally, which of the following solutions and services are in place in your company?

All respondents/Several answers possible



14.9 solutions on average



“opinionway for CESIN

*New item
** Changed item

↗ ↘ Statistically significant change compared to the previous wave

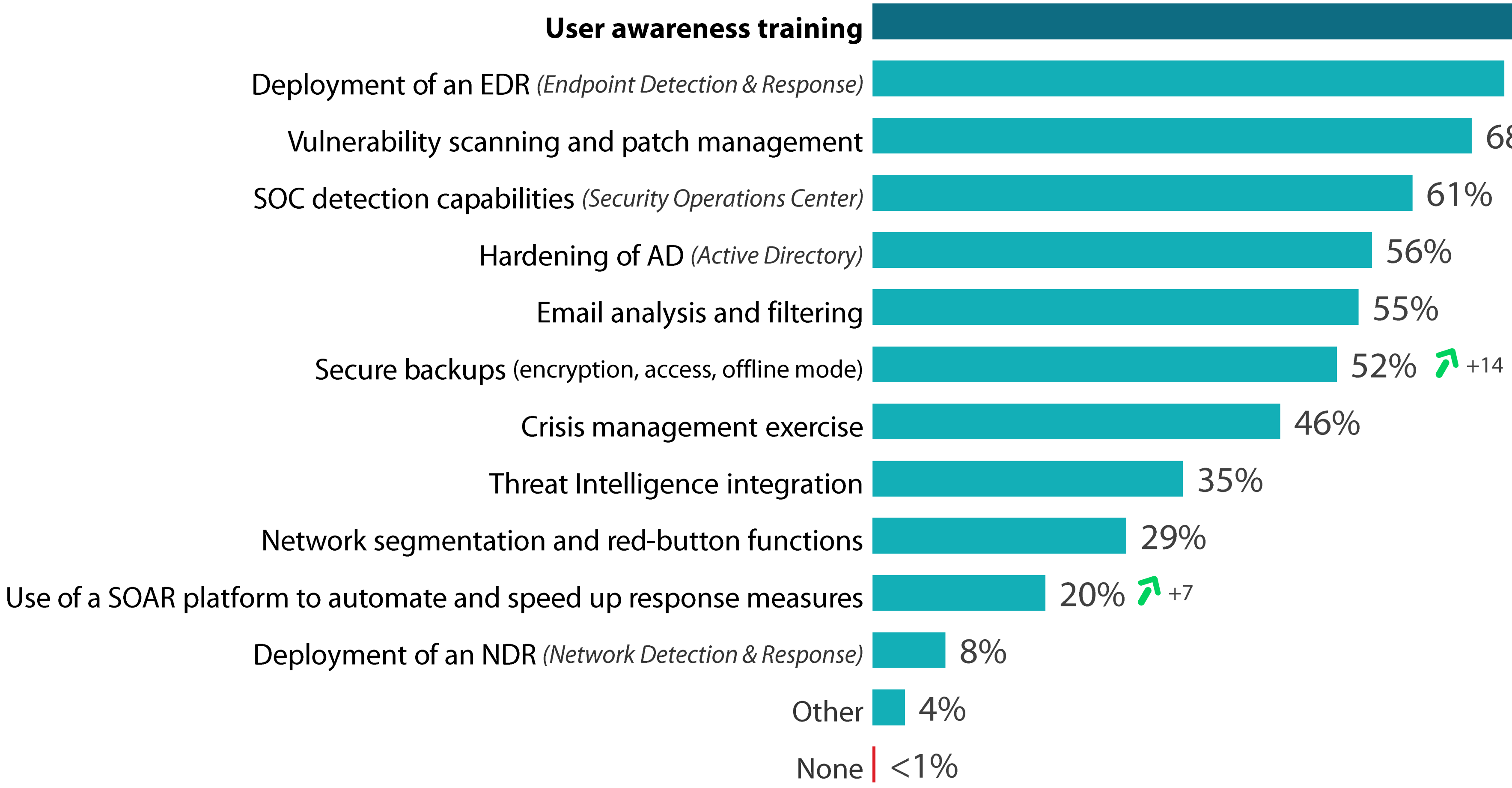
Changes should be interpreted with caution due to the addition of items

In addition to raising awareness, CISOs are massively deploying the tools considered as the most effective: EDR, vulnerability management tools and SOC services. The efforts made in terms of resilience, particularly with regard to the security of backups, have also been noted

Q11. In response to this wave of cyberattacks dominated by ransomware, what measures have you reinforced?

All respondents/Several answers possible

328 people



5.9 ↗ +0.4

devices
on average

“opinionway for CESIN

↗ ↘ Statistically significant change compared to the previous wave

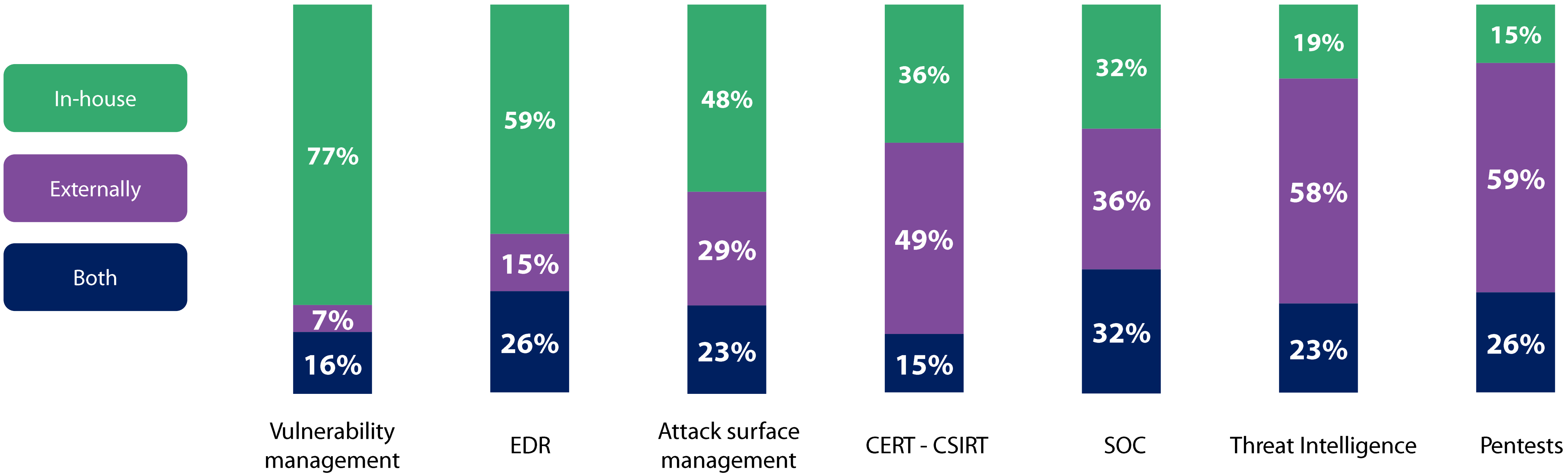
Although vulnerability management is still mainly internal, it should be noted that there is a significant proportion of outsourcing of services, particularly for EDR or attack surface management, which are solutions that are often acquired with the associated operational services

New question

Q30b. How do you operate the following solutions and services?

Respondents: solution in place in the company

328 people



Service not in place	7%	12%	42%	27%	20%	37%	7%

"opinionway for CESIN

Companies believe that they have the means to protect themselves from a large-scale cyberattack with protection and detection means. However, they remain limited in their ability to respond or rebuild after an attack

328 people

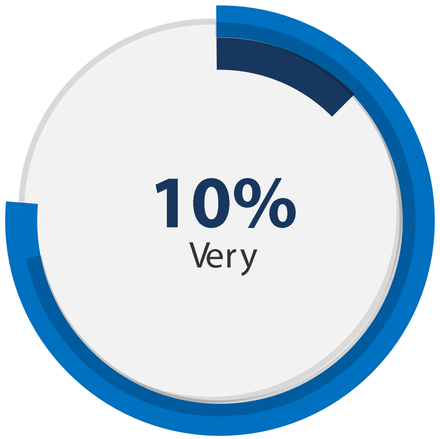
Q14. In your opinion, is your company prepared to handle a large-scale cyberattack in terms of...?

All respondents

Changed item

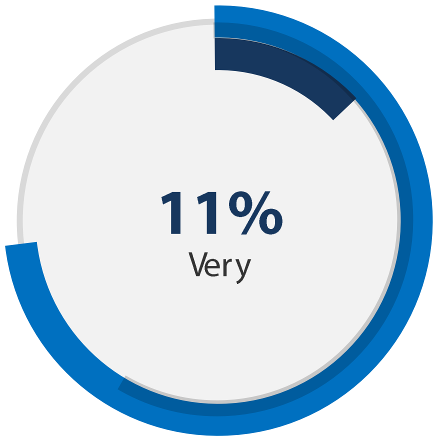
77%

Means of prevention



70%

Means of detection

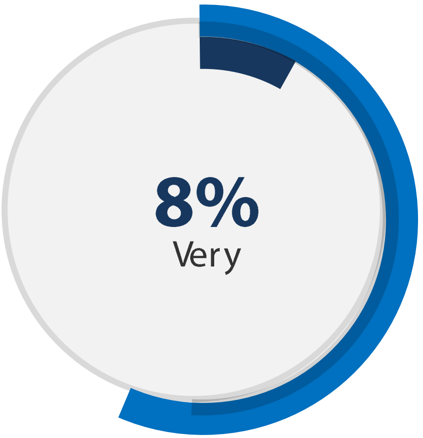


Reminder Wave 7: 72%

Changed item

58%

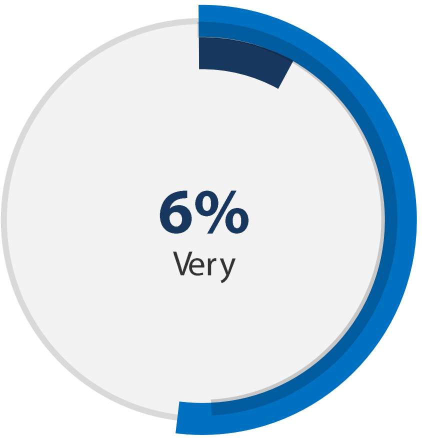
Response to the attack



Changed item

53%

Reconstruction after the attack

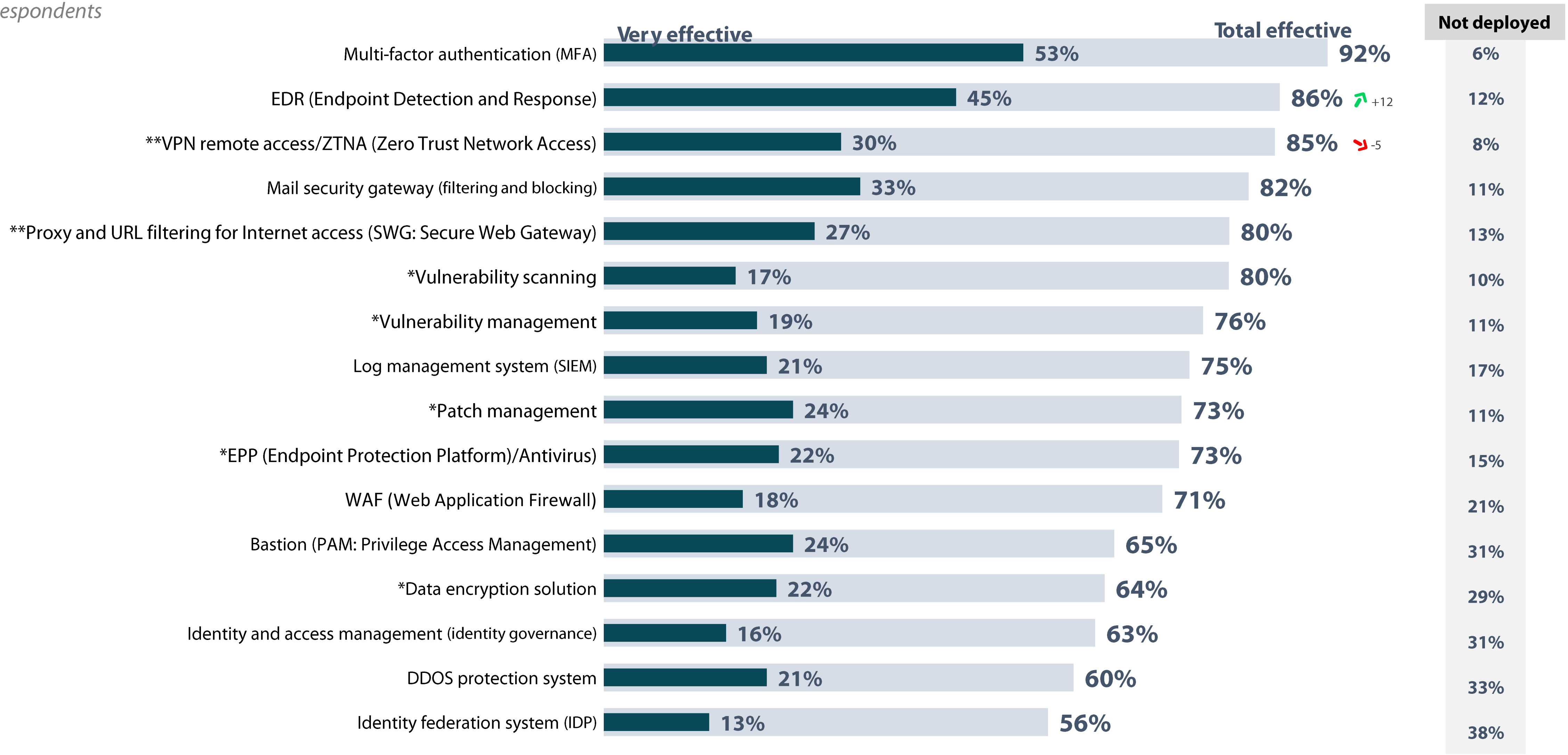


There is a plebiscite for the MFA/EDR pair, which are considered the two most effective solutions in the current context, and the confidence in the EDR has increased again in 2022

328 people

Q13. Do you think each of the following solutions is very effective, somewhat effective, not very effective or not at all effective?

All respondents



"opinionway for CESIN

*New item
** Changed item

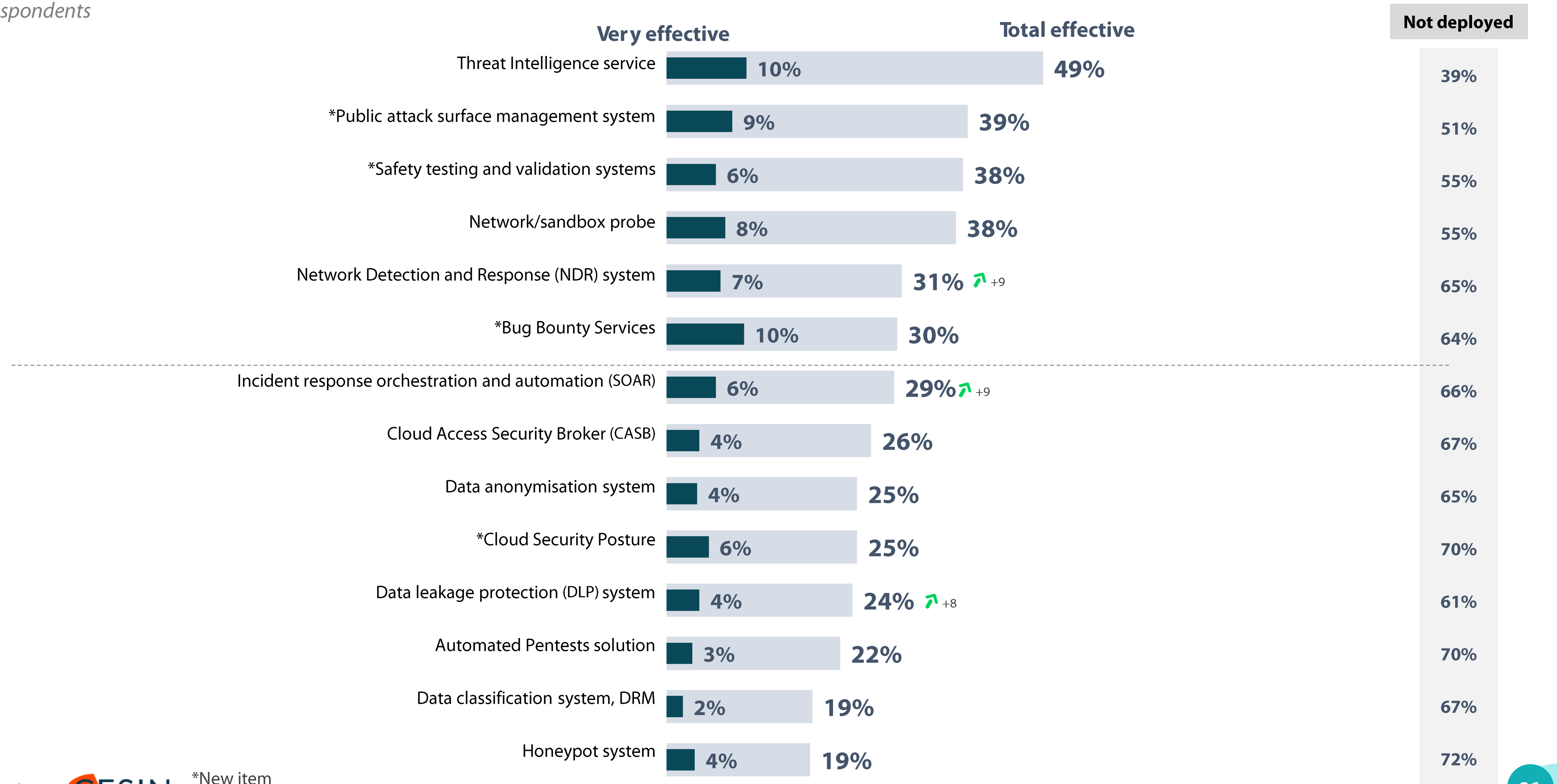
↗ ↘ Statistically significant change compared to the previous wave
Changes should be interpreted with caution due to the addition of items

The effectiveness of the other solutions is somewhat lower, which can be explained by the lower deployment of these solutions

328 people

Q13. Do you think each of the following solutions is very effective, somewhat effective, not very effective or not at all effective?

All respondents



*New item
** Changed item

↗ ↘ Statistically significant change compared to the previous wave

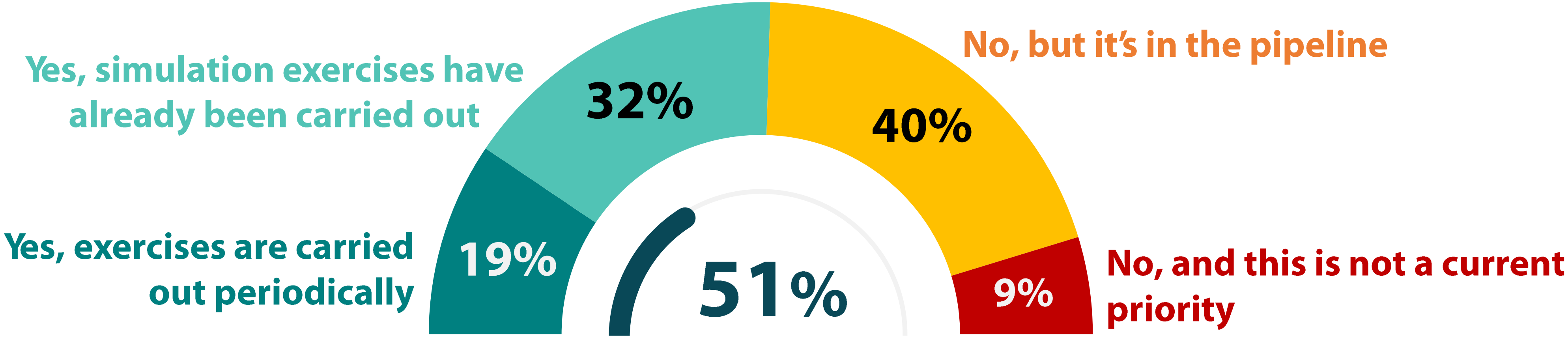
Changes should be interpreted with caution due to the addition of items

Half of all companies have a cyber crisis training programme in place, a number that is growing year on year

328 people

Q15. Does your company have a cyber crisis training programme in place?

All respondents



HAVE SET UP A CYBER CRISIS TRAINING PROGRAMME

Reminder Wave 7: 44%

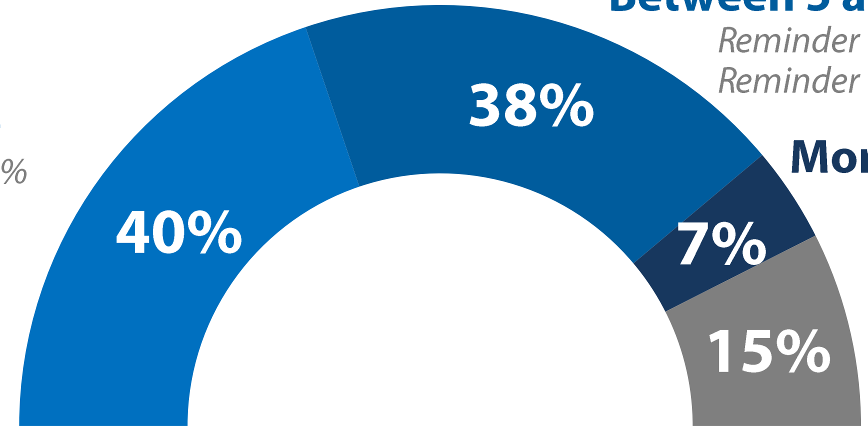
↗ ↘ Statistically significant change compared to the previous wave

Cyber budgets are maintained or even slightly increased and the majority of budgets are above 5% of the IT budget

328 people

Q18. In your company, how much of the IT/digital budget is spent on security?

All respondents



Less than 5%
Reminder Wave 7: 40%

Between 5 and 10%.
Reminder Wave 7: 36%
Reminder Wave 6: 26%

More than 10%
Reminder Wave 7: 8%

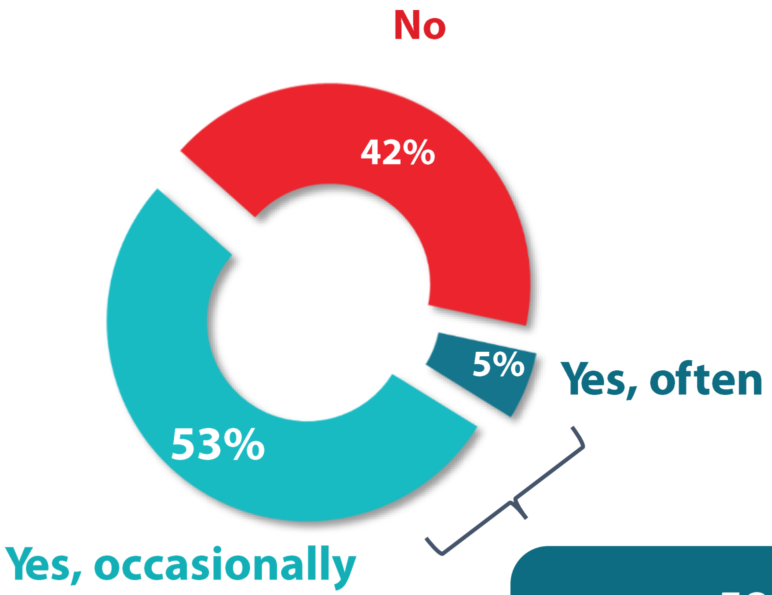
5% or more : 45%
Reminder Wave 7: 44%

Don't know
Reminder Wave 7: 16%

Almost 6 out of 10 companies use start-up solutions

328 people

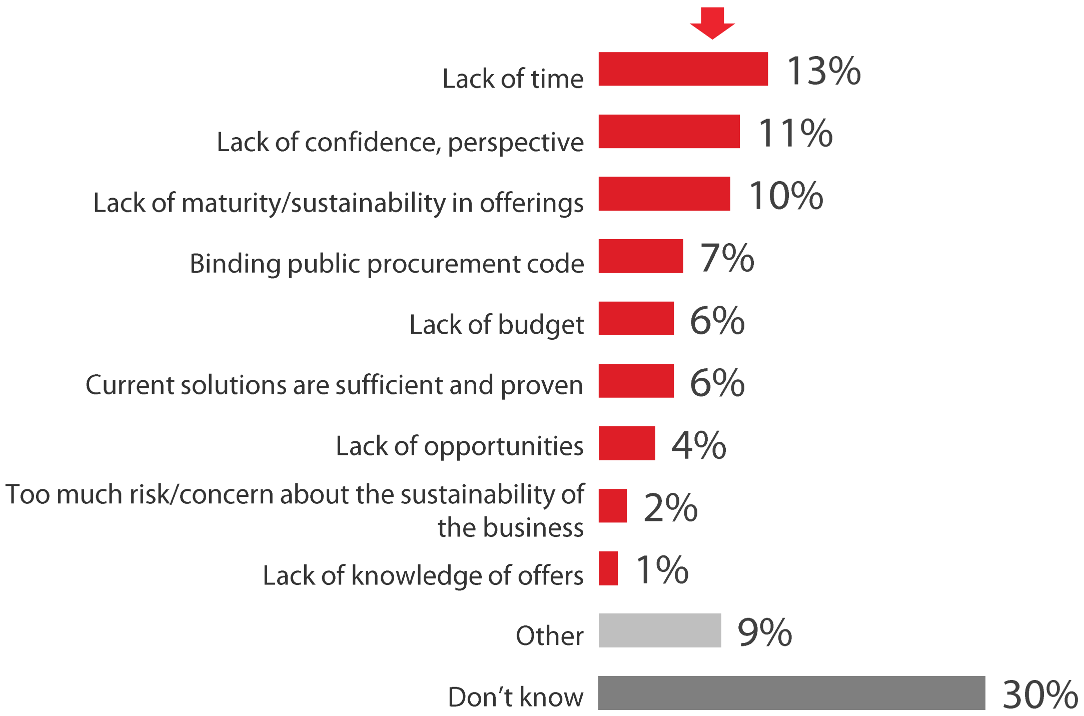
Q26. In terms of cybersecurity, do you make use of innovative offers from start-ups? *All respondents*
Q26a. Why not? *Respondents: do not use offers from start-ups (137)*



58% use innovative offers from start-ups

Reminder Wave 7: 62%

42% do not use such offers



“opinionway for CESIN

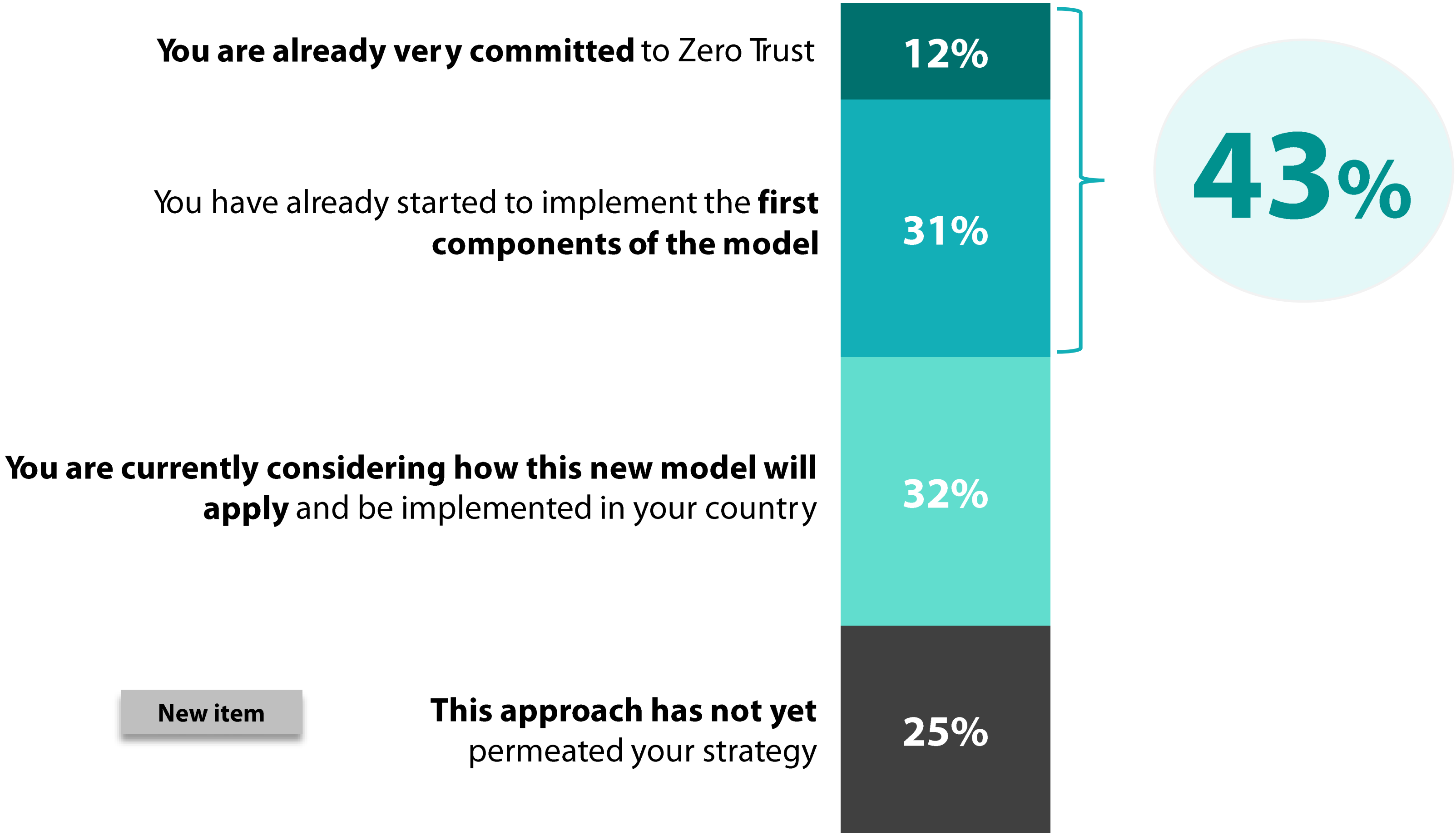
The Zero Trust concept is beginning to be implemented in companies, although a quarter are still lagging behind

328 people

Modified question

Q28. What is your vision of the Zero Trust concept?

All respondents



You are already very committed to Zero Trust 12%

You have already started to implement the **first components of the model** 31%

43%

You are currently considering how this new model will apply and be implemented in your country 32%

New item

This approach has not yet permeated your strategy 25%

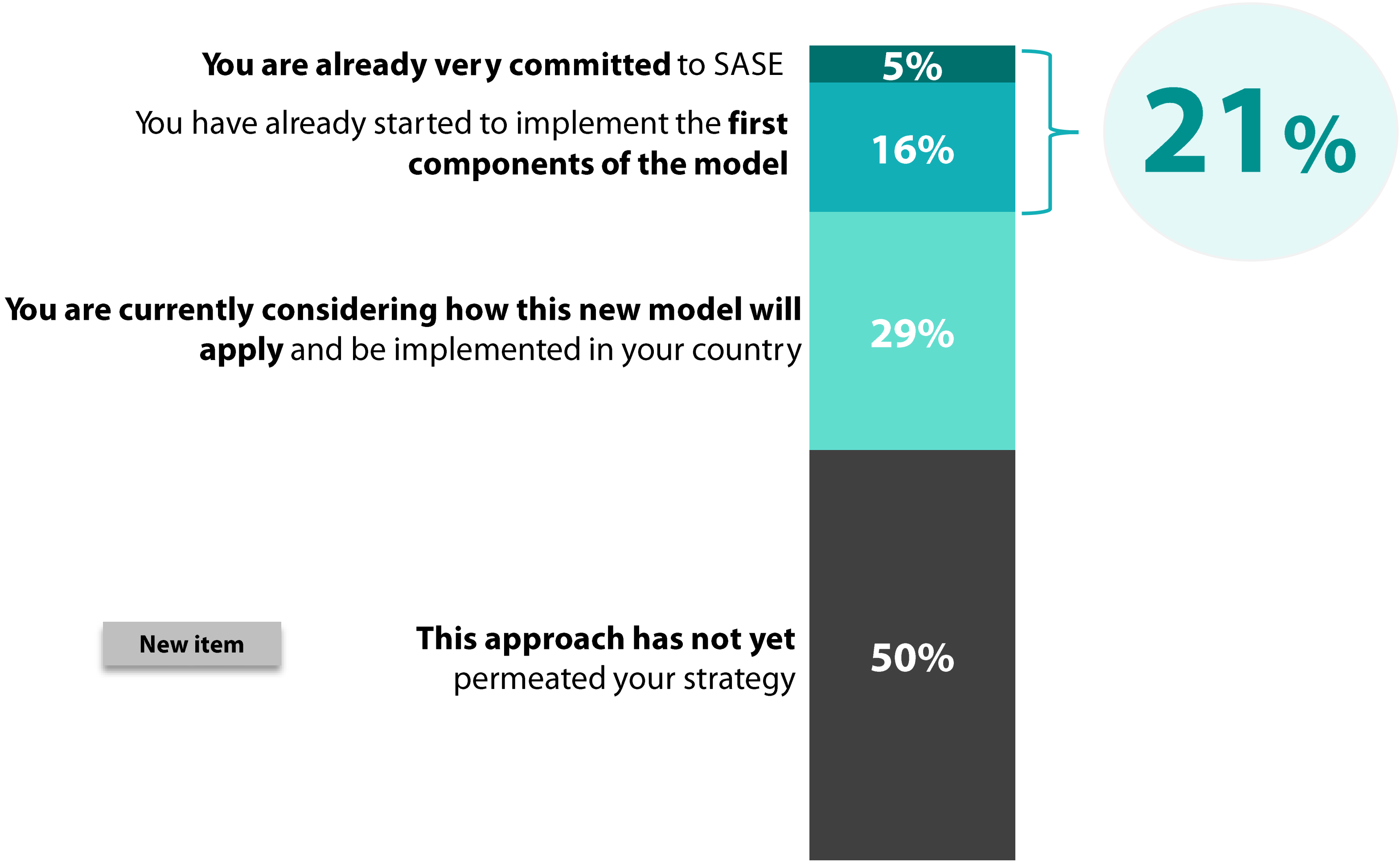
The SASE concept does not yet seem to have permeated companies

328 people

Modified question

Q34. What is your vision of the SASE concept?

All respondents



New item

“opinionway for CESIN

Focus on…

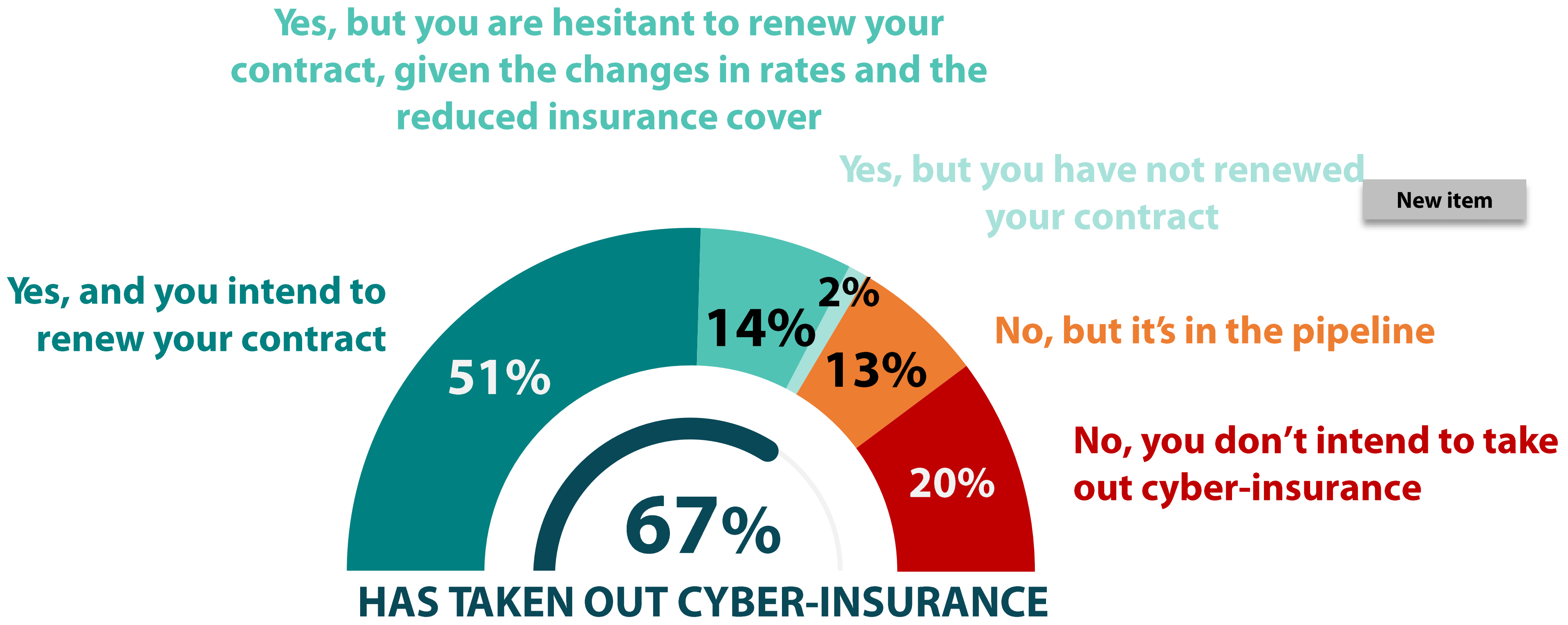
Cyber-insurance

Two-thirds of companies have taken out cyber-insurance, however more than 1 in 10 are reluctant to renew their policy, and 2% of companies have already given it up

328 people

Q31. Have you taken out cyber-insurance?

All respondents



Three quarters of insured companies have never used their cyber-insurance

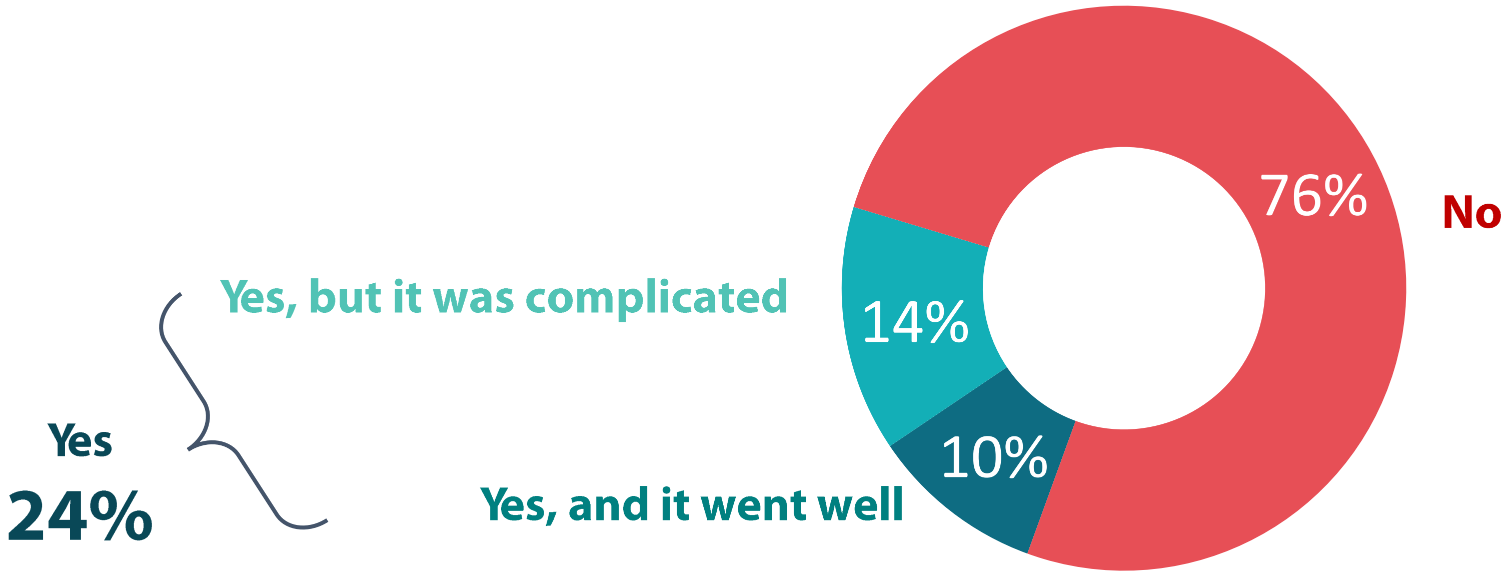
220 people

Modified filter

Q32. Has your company ever used its cyber-insurance in the event of a cyberattack?

Respondents have or are planning to have cyber insurance

Use of cyber-insurance



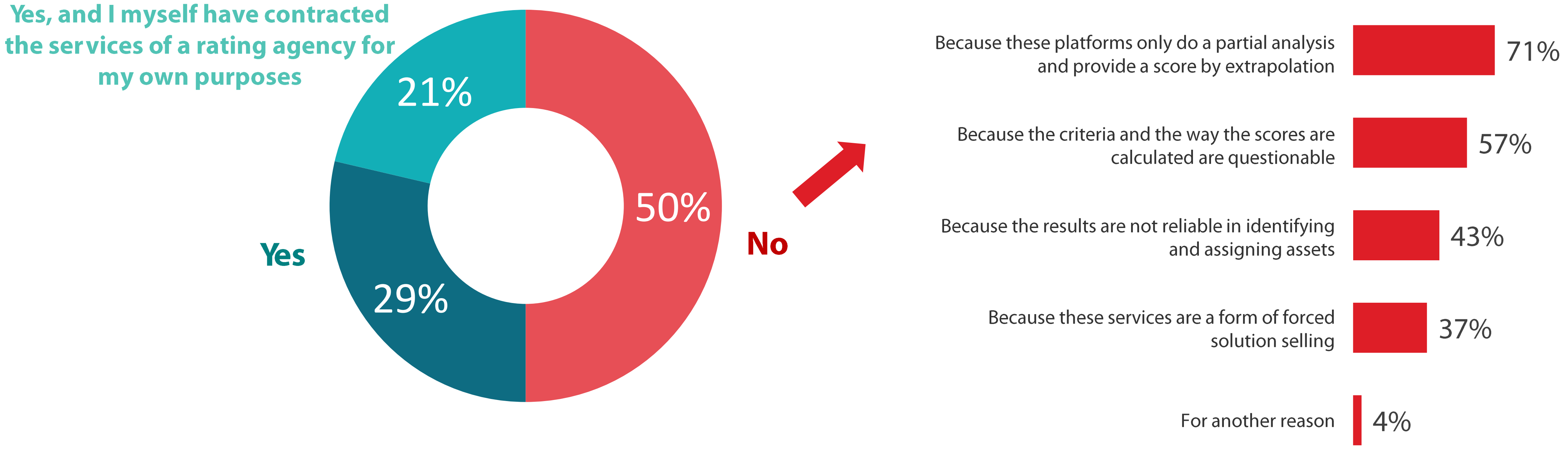
The use of rating agencies for e-insurers convinces only half of the companies. Others highlight the questionable quality of the analyses

328 people

Modified question

Q33. E-insurers are increasingly using the services of rating agencies. Is this a good thing in your opinion? *All respondents*
Q33bis. Why? *"It is not a good thing" respondents (164)*

Use of the rating agency service



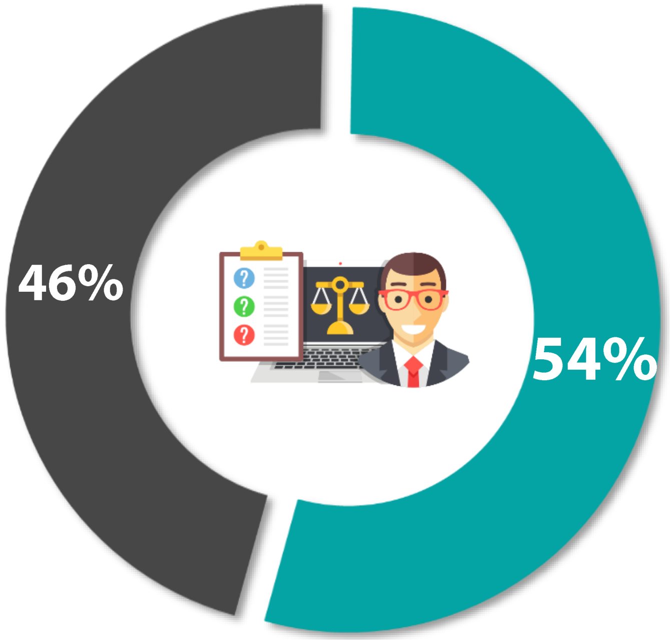
As for 2021, almost half of the companies that have suffered an attack have already filed a complaint...

147 people

Q8. Have you filed a complaint as a result of the cyberattack(s) on your company?

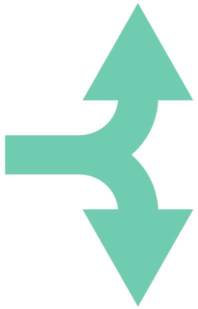
Respondents having reported an attack

45% of companies suffered at least one cyberattack in 2022



Filed a complaint

Reminder Wave 7: 50%



for **all attacks**: **27%**

for **some attacks**: **27%**

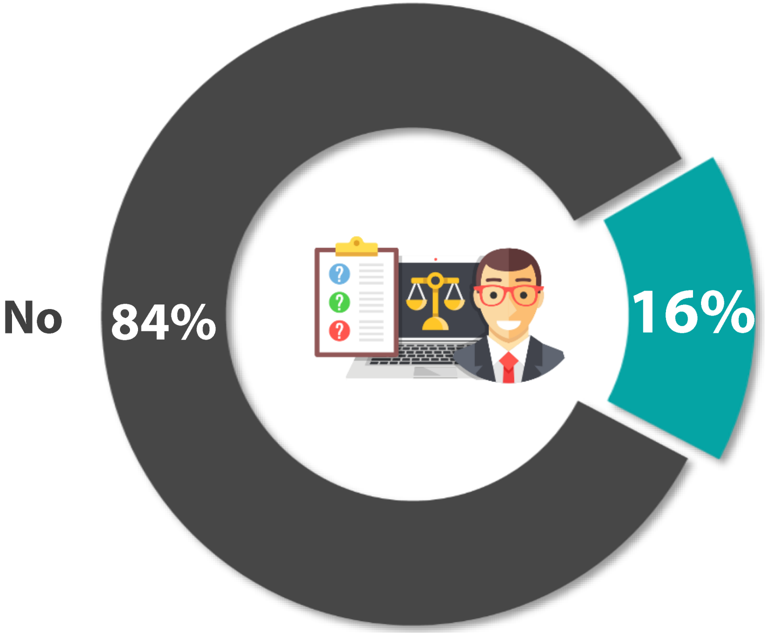
...but identification/interrogation of attackers rarely occurs

80 people

Q8a. As a result of your complaint(s), did the investigation lead to the identification and/or arrest of the attacker(s)?

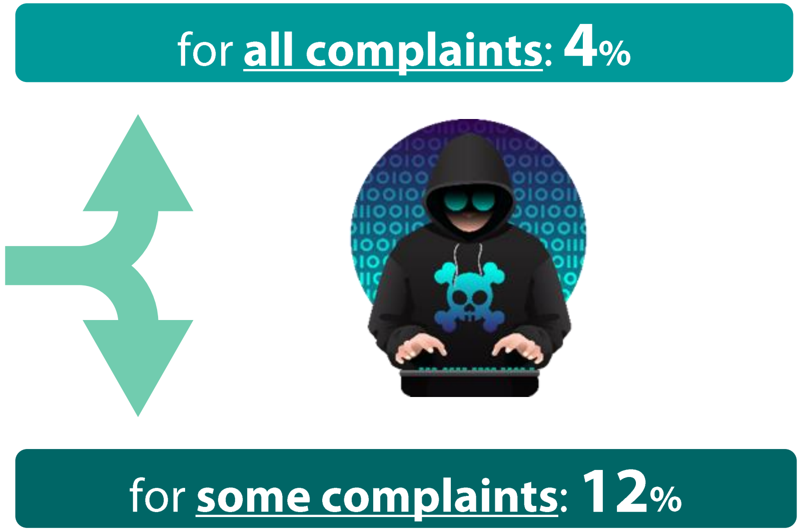
Respondents having complained

54% of companies have filed a complaint



Yes, the investigation led to an identification

Reminder Wave 7: 16%



for **all complaints**: **4**%

for **some complaints**: **12**%

03

Employees are aware, but must now apply the recommendations, especially those related to the Cloud

While companies carry out cyber-risk awareness actions for a large number of users, only 2/3 follow the recommendations

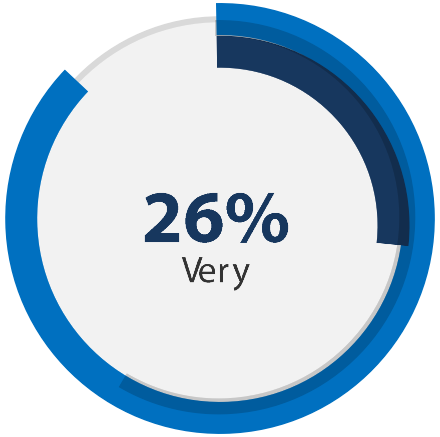
328 people

Q19. With regard to employee awareness and training in cybersecurity issues, do you think that…?

All respondents

85%

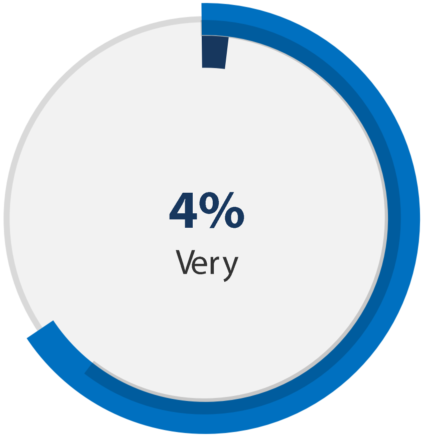
Users **are aware of** cyber risks



Reminder Wave 7: 82%

66%

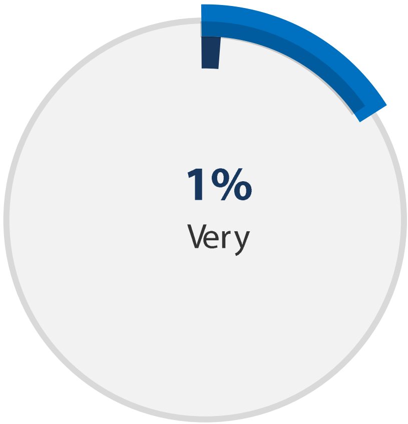
Users **comply with recommendations**



Reminder Wave 7: 70%

17%

Users **take precautions that go beyond the recommendations** given



Reminder Wave 7: 18%

Although administrators, architects and developers seem to have been made aware of this, they nevertheless lack expertise in the area of security

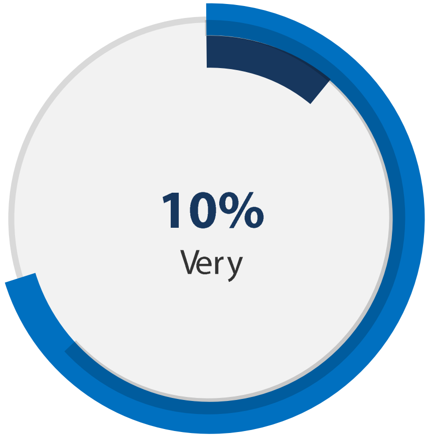
328 people

Q19. With regard to employee awareness and training in cybersecurity issues, do you think that…?

All respondents

70%

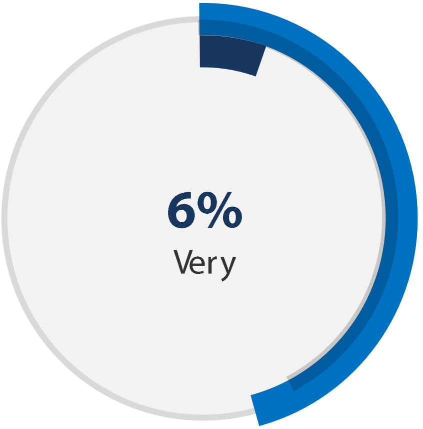
Administrators, architects and developers are aware of and apply good security practices in terms of operations, design and development



Reminder Wave 7: 68%

47%

Administrators, architects and developers have sufficient training and have acquired the necessary expertise, especially in new technology



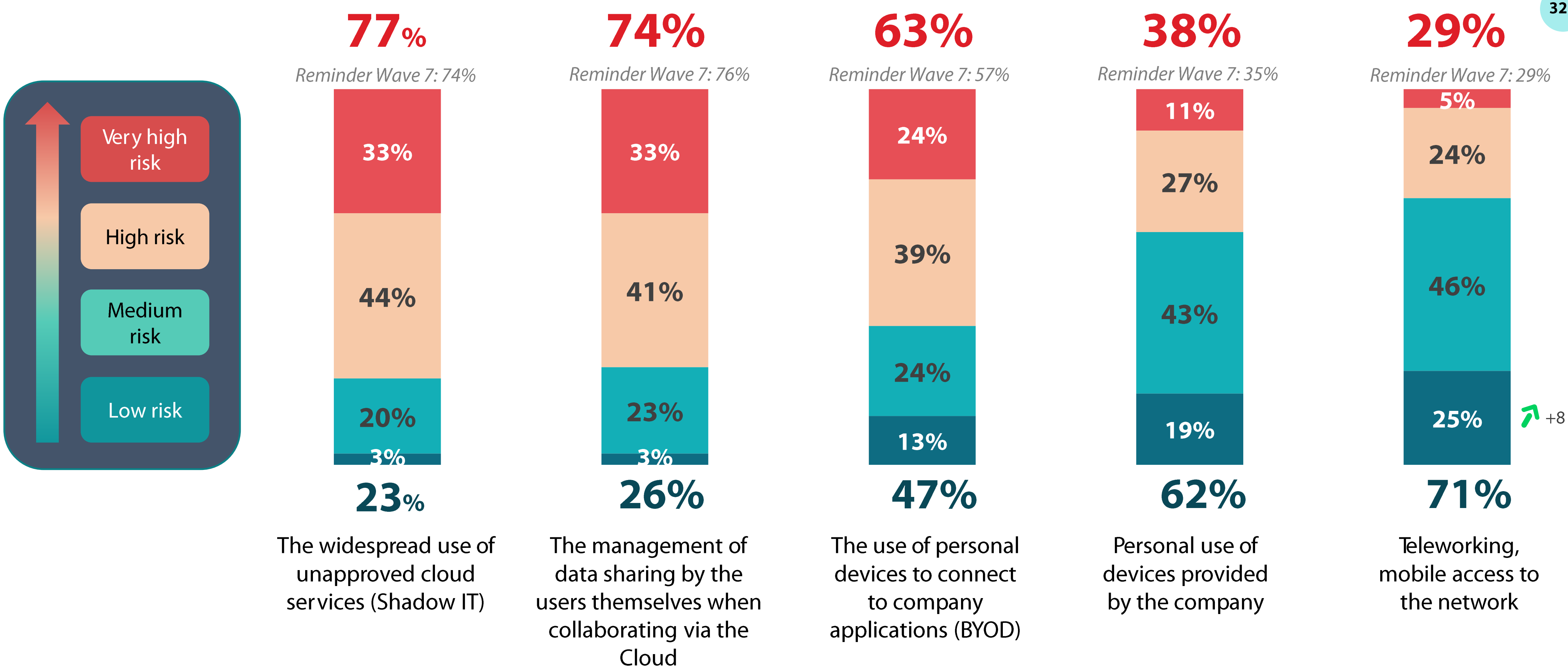
Changed Item

Similar to 2021, the digital uses perceived as the most risky this year are around the Cloud through Shadow IT and data exposure by users. Risks related to teleworking and personal use of work equipment now seem to be better controlled

Q23. How do you assess the level of risk induced by the following digital uses by employees?

All respondents

328 people



Statistically significant change compared to the previous wave

The risk factors in the use of the Cloud lie first of all in the lack of control of the hosting provider's subcontracting chain and the difficulty of controlling access by the host provider's administrators

328 people

Q21. In your opinion, do the following factors represent a low, moderate or high risk with regard to the use of the cloud?

All respondents

Reminder Wave 7 Top 5		% A strong risk	
1	●	**51%**	**Lack of control of the hosting company's subcontracting chain**
2	●	**49%**	**Difficulty in controlling access by the host's administrators**
3	●	43%	Expertise still too rare, expected from architects and administrators
	●	42%	Data storage in France/Europe but handled and/or operated by foreign providers where the law of the country of origin also applies
	●	40%	Difficulty in conducting audits (pentesting, configuration control, site visits)
4	●	40%	Poor visibility of the cloud's inventory of resources
	●	37%	Storage of data in data centres abroad, outside French law
	●	36%	Failure of the hosting company to delete data at the end of the contract (normal or early), despite being contractually required
	●	35%	Lack of control over security settings/weak encryption by the hosting company
	●	35%	Difficulty in controlling how it is used by your company's employees
	●	32%	Difficult or impossible to feed the SIEM with logs from the Cloud
	●	32%	Data/application unavailable due to an attack on the host
	●	32%	High frequency of new releases with potential uncontrolled changes in security principles or parameters
5	●	31%	Confidentiality of data vis-à-vis the hosting company
	●	31%	Failure to erase data during use, as deletions and purges by the customer are not really effective
	●	29%	Bounce attack from the host
	●	27%	Lack of compartmentalisation between the various clients of the hosting company
	●	27%	Processing and use of data by the host without the knowledge of its customers
	●	26%	Systemic propagation of any attacks and human errors that could occur at the hosting company
	●	23%	Failure of the hosting company to return data at the end of the contract (normal or early) when contractually required
	●	16%	Trapping a hosted application

CISOs believe that specific tools are needed to monitor the Cloud, not necessarily those offered natively by Cloud Providers

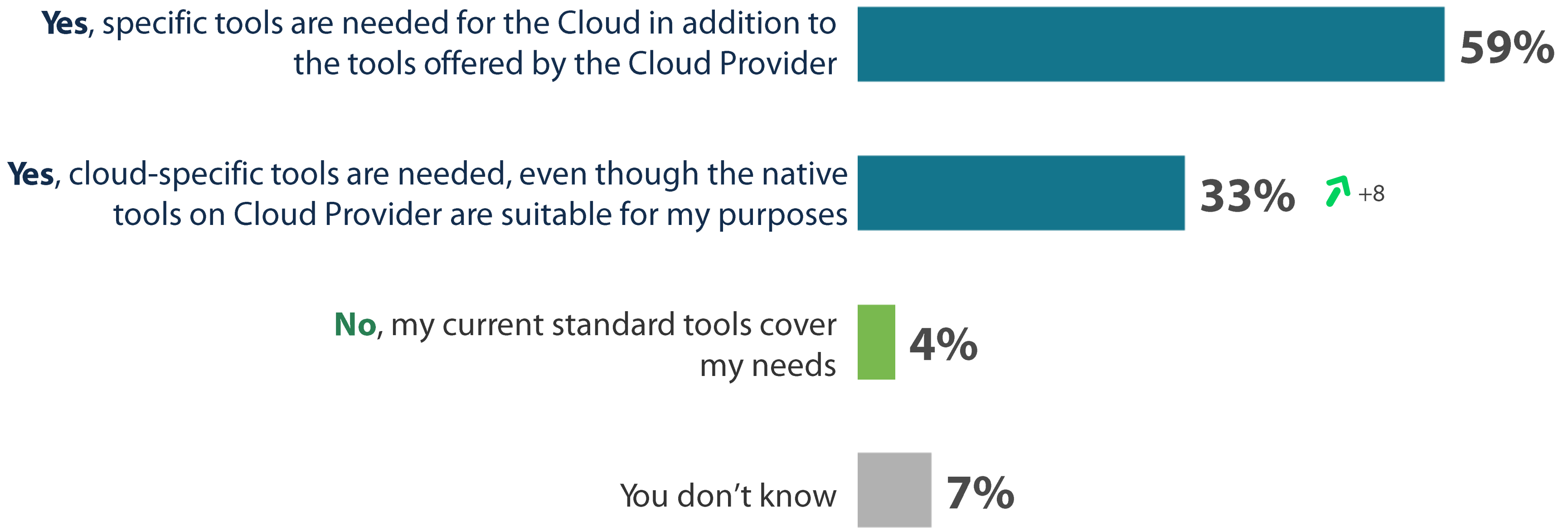
Q22. Do you think that securing data stored in the cloud requires specific tools or devices?

All respondents

328 people

… 89% believe that securing data stored in the cloud requires specific tools

Reminder Wave 7: 86%



↗ ↘ Statistically significant change compared to the previous wave

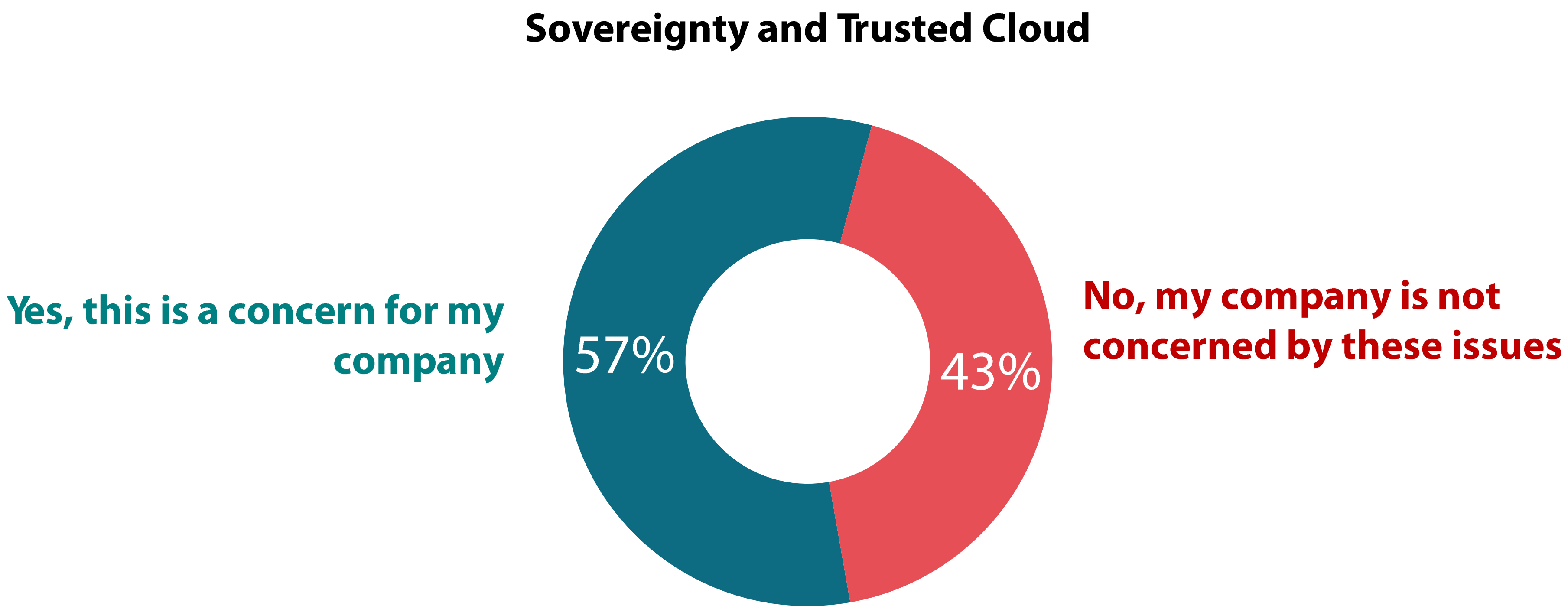
opinionway for CESIN

Sovereignty and Trusted Cloud issues are of concern to nearly 6 out of 10 companies

328 people

Q35. Many initiatives have recently been launched in the area of sovereignty and the Trusted Cloud. Do you feel concerned by these issues?

All respondents



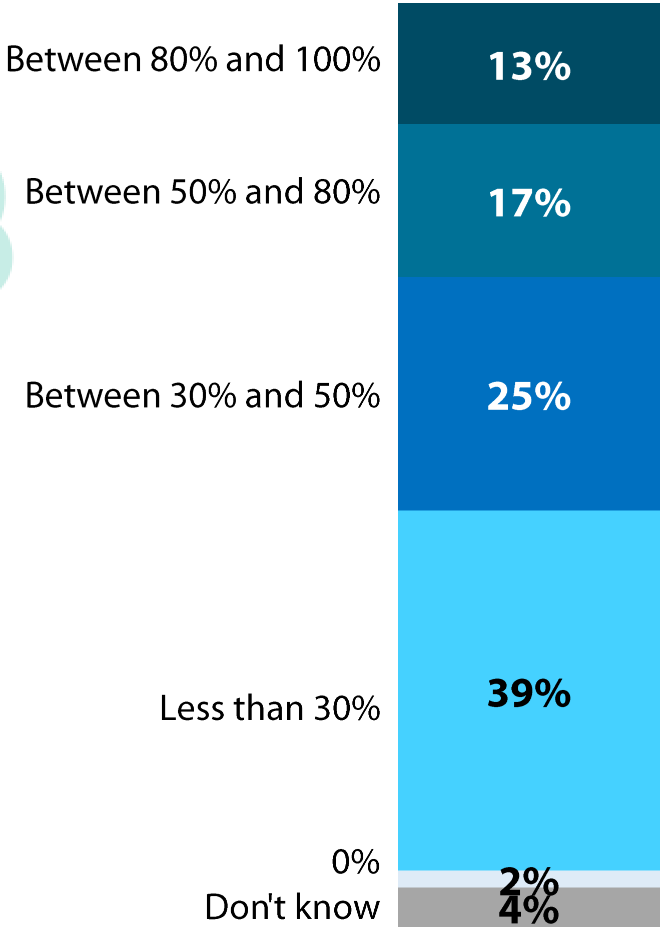
The cloud still represents less than 50% of the IS in many companies

328 people

Modified question

Q20. What is the degree of penetration of your IS in the Cloud, whether in IaaS, PaaS or SaaS mode?

All respondents



“opinionway for CESIN

04

Cybersecurity remains a key issue for companies

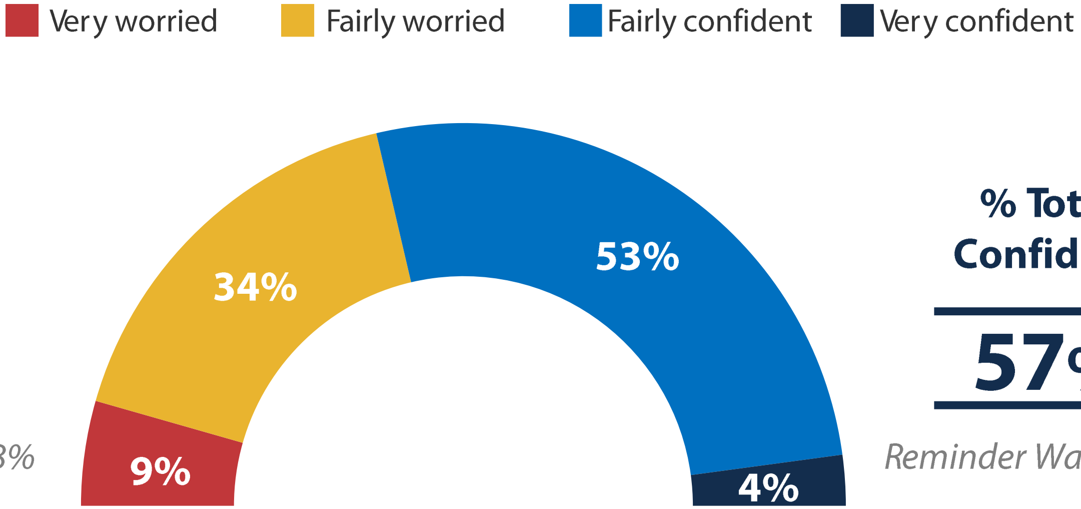
Companies are still concerned about their ability to deal with cyber risks in the future, although confidence is on the rise

328 people

Q24. For the future, would you say you are very confident, fairly confident, fairly worried or very worried about...?

All respondents

Your company's **ability** to deal with cyber risks



% Total Worried

43%

Reminder Wave 7: 48%

% Total Confident

57%

Reminder Wave 7: 52%

"opinionway for CESIN

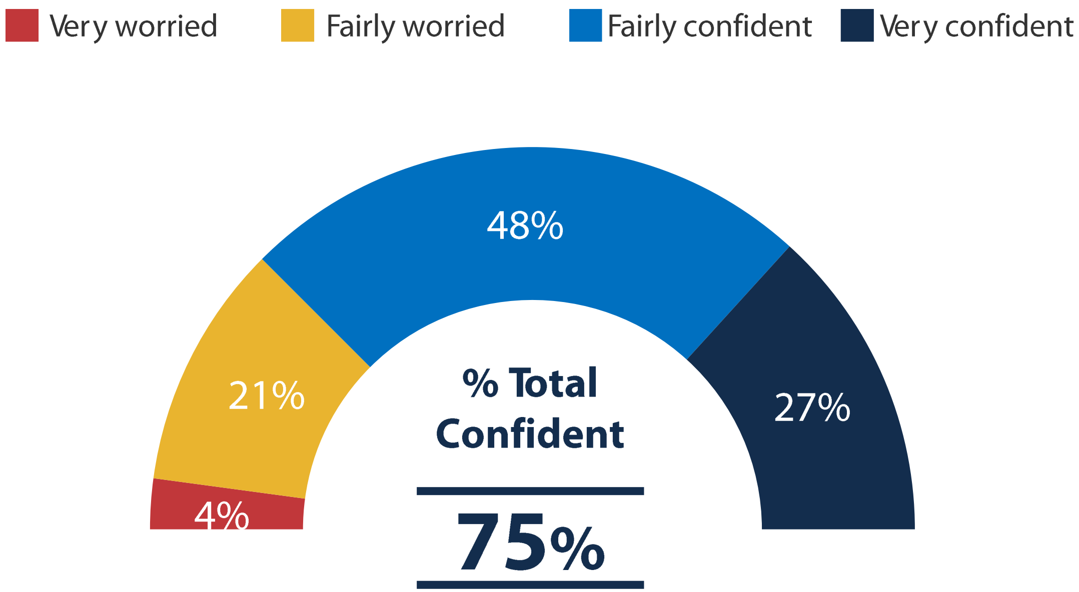
Cybersecurity is perceived as an important issue and taken into account within the COMEX

328 people

Q24. For the future, would you say you are very confident, fairly confident, fairly worried or very worried about...?

All respondents

The **consideration of cybersecurity issues** within your company's executive committee



Reminder Wave 7: 79%

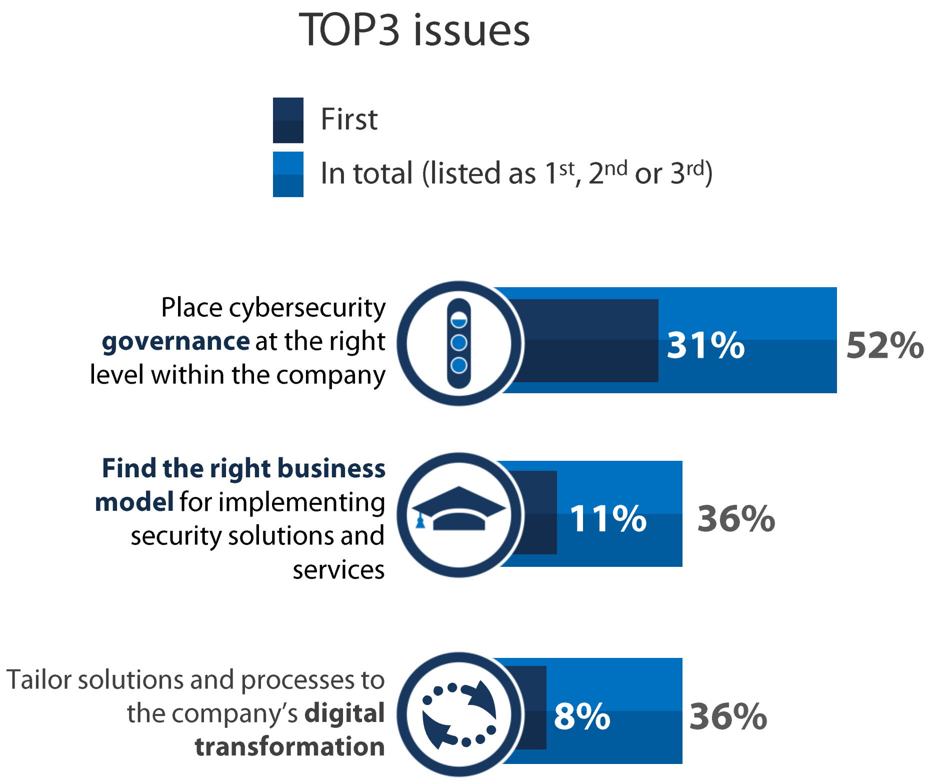
The main issue for the future with regard to cybersecurity lies in the proper structuring of corporate cybersecurity governance.

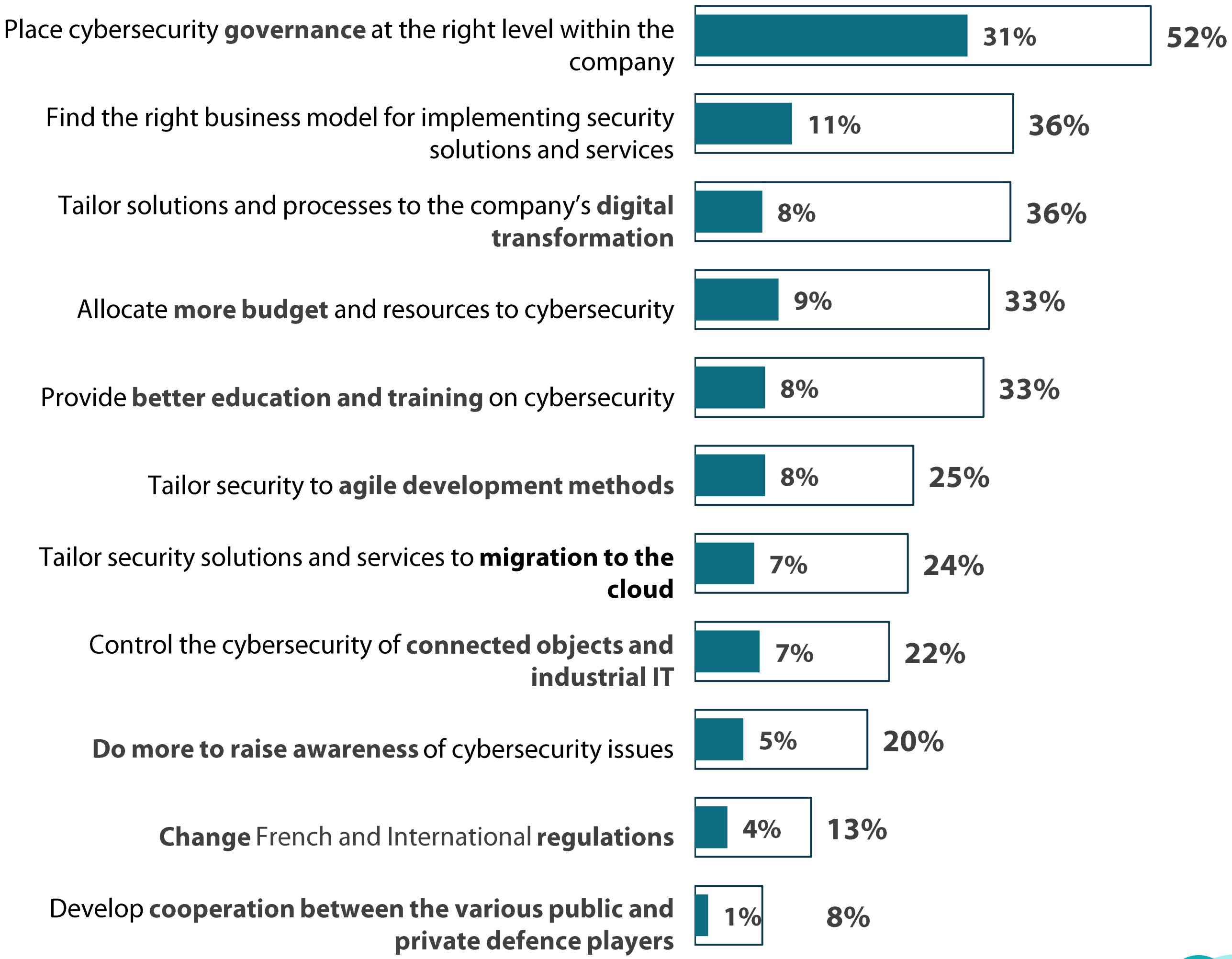
328 people

Changed Item

Q27. Of the following issues, what do you think are the three most important for the future of corporate cybersecurity?

All respondents





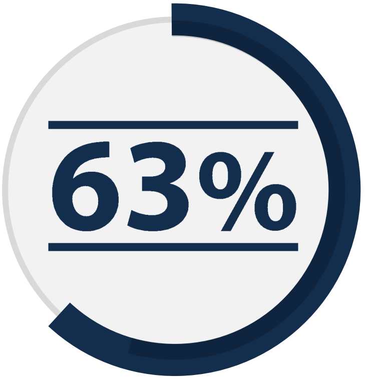
In this context, almost 2/3 of companies expect to increase their budgets for protection against cyber risks, a lower proportion than in 2021

328 people

Q17. Over the next 12 months, does your company plan to...?

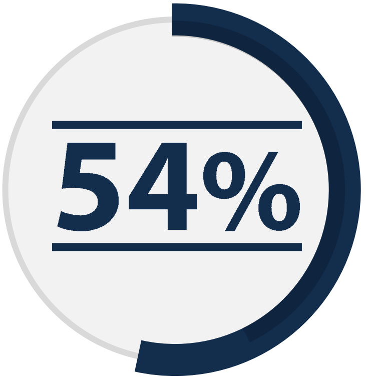
All respondents

increase budgets for protection against cyber-risks



Reminder Wave 7: 70%

increase the number of staff allocated to protection against cyber-risks



Reminder Wave 7: 56%

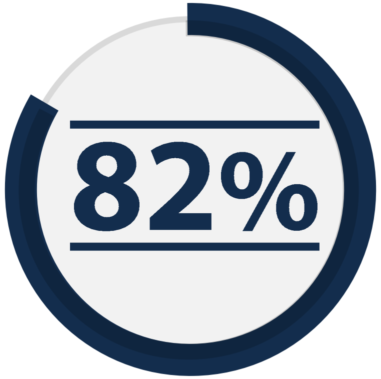
More than 8 out of 10 companies plan to acquire new protection solutions

328 people

Q17. Over the next 12 months, does your company plan to...?

All respondents

acquire new technical solutions for cybersecurity



Reminder Wave 7: 84%

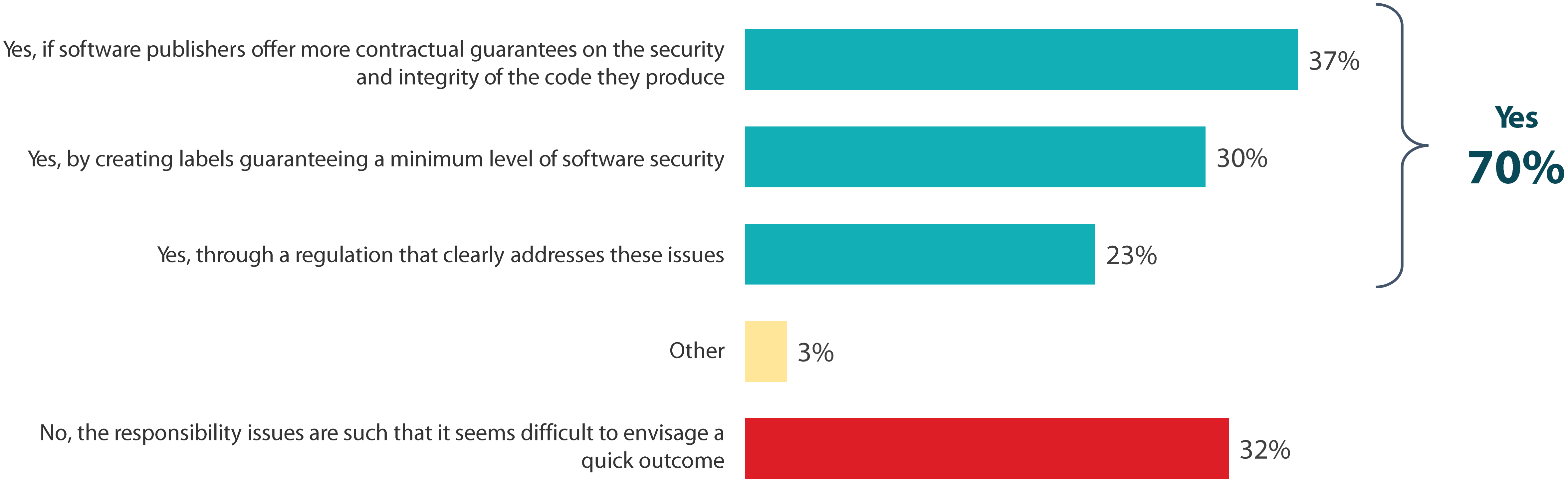
Most companies believe that supply chain security issues can be resolved, provided there are greater assurances for code and labels

Modified items

Q36. Solarwinds attacks raise the question of software security. Do you think these supply chain security issues can be resolved?

All respondents/Several answers possible

328 people



Conclusion

A downward trend in cyberattacks

A downward trend is confirmed: 45% of companies report having suffered at least one attack in 2022

The proportion of companies reporting that they have suffered at least one impactful cyberattack in 2022 has been falling for several years (54% in 2021 and 57% in 2020 and 65% in 2019), but it is still almost 1 in 2.

A drop in the number of successful cyberattacks can be explained by the various prevention, protection and detection/response measures that have been put in place and are now bearing fruit.

Phishing or spear phishing remains the main attack vector. Cyberattacks mainly lead to data theft and identity theft, which ultimately have a fairly strong impact on companies' business (60%), particularly through production disruptions.

User awareness at the heart of the fight against cyberattacks

For more than 8 out of 10 companies, the 1st step in reducing the risk of cyberattacks is to raise user awareness.

Cyber-risk awareness actions are widely offered to users, although only two thirds of them follow the recommendations.

Administrators, architects and developers seem to have been made aware of this, even if they lack expertise in this area.

Furthermore, it should be noted that cyber crisis training programmes are increasingly successful (51% in 2022 and 44% in 2021 and 33% in 2020).

Intensification of the solutions put in place to combat cyberattacks

A wide range of cybersecurity solutions in place, with greater deployment of EDR

Today, companies have multiple solutions and services to combat cyberattacks. Furthermore, there is an increasing emphasis on rapid detection and response tools, such as EDR (81%, +13 points) and NDR (21%, +8 points).

CISOs are reinforcing tools considered as the most effective, such as EDR, vulnerability management tools and SOC services.

Cyber insurance with limited profits

Almost 2/3 of companies have taken out cyber insurance. However, just under 1 in 5 are reluctant to renew their policy, a finding that may be explained by the low take-up of their cyber insurance.

Furthermore, the use of rating agencies does not seem to give more legitimacy to e-insurers.

Cloud data to be secured

Digital uses around the Cloud constitute a major risk (77%) according to the CISOs.

The degree of penetration the IS of companies in the cloud is still a minority: less than 50% for nearly 2/3 of them. Indeed, its use may be perceived as risky, especially with regard to factors such as the lack of control over the hosting provider's subcontracting chain or the difficulty of controlling access by the hosting provider's administrators.

In this context, almost all CISOs (89%) believe that the use of the Cloud must be accompanied by specific tools for its monitoring, not necessarily offered by Cloud Providers.

Still a key issue for tomorrow

Cybersecurity: a future issue for companies

Even if the proportion of companies that are victims of cyberattacks is falling, there is still concern:

- 50% believe that the threat of cyber espionage in their company is high
- 43% say they are concerned about their ability to deal with cyber risks, a significant proportion although confidence is on the rise (57% vs. 52% in 2021).

In the same way as in 2021, companies are fairly confident about their ability to protect themselves from a large-scale cyberattack, but they are uncertain about their ability to respond or rebuild after an attack.

It is also in this context that most companies are considering taking cybersecurity issues into account within their COMEX, because the main objective for tomorrow's cybersecurity lies in the proper structuring of governance of this issue within the company.

MAKE THE WORLD EASY TO UNDERSTAND SO WE CAN ACT NOW AND IMAGINE THE FUTURE.

WE ARE DIGITAL !

Founded in 2000 on this radically innovative idea at the time, OpinionWay was a forerunner in renewing the practices of the marketing and opinion researches.

With continuous growth since its creation, the company has constantly opened up to new horizons to better address all marketing and societal issues, by integrating Social Media Intelligence, smart data exploitation, creative co-construction activities, online communities approaches and storytelling into its methodologies.

Today OpinionWay continues its dynamic growth by expanding geographically in high-potential regions such as Eastern Europe and Africa.

This is the mission that drives OpinionWay's employees and the foundation of the relationship they build with their clients.

The pleasure they derive from providing answers to the questions they ask themselves, reducing uncertainty about the decisions to be made, tracking relevant insights and co-constructing solutions for the future, feeds all the projects they work on.

This enthusiasm, combined with a genuine taste for innovation and transmission, explains why our customers express a high level of satisfaction after each collaboration - 8.9/10, and a high recommendation rate – 3,9/4.

Pleasure, commitment and intellectual stimulation are the three mantras of our interventions.

LET'S STAY CONNECTED !

www.opinion-way.com

Let's go further together !

Receive our latest market researches results each week in your mailbox by subscribing to our newsletter !

“opinionway

15 place de la République
75003 Paris

PARIS
CASABLANCA
ALGER
VARSOVIE
ABIDJAN